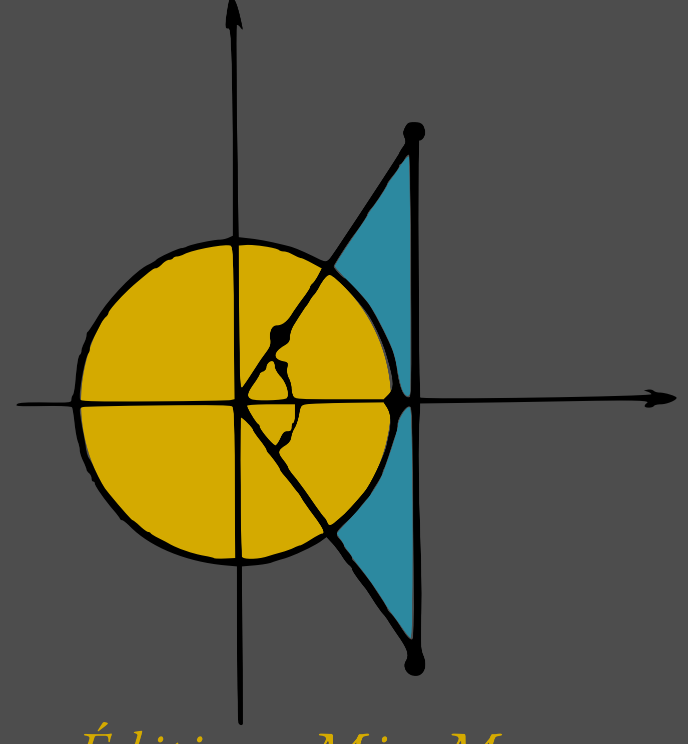
A. Kurosh

Cours d'Algèbre Supérieur



Éditions Mir Moscou

А. Г. КУРОШ

КУРС ВЫСШЕЙ АЛГЕБРЫ

ИЗДАТЕЛЬСТВО «НАУКА»
МОСКВА

A. KUROSH

COURS D'ALGÈBRE SUPÉRIEURE

ÉDITIONS MIR • MOSCOU

UDC 512.8=40

TRADUIT DU RUSSE

На французском языке

K $\frac{0223-379}{041(01)-73}$

TABLE DES MATIÈRES

PRÉFACE

Le « Cours d'algèbre supérieure » du professeur Alexandre Kurosh que nous recommandons à l'attention du lecteur est la traduction en langue française d'une œuvre bien connue en Union Soviétique de cet auteur.

La connaissance de l'algèbre supérieure est nécessaire à la formation des étudiants qui veulent se consacrer aux mathématiques.

Le livre que nous présentons donne un moyen relativement rapide de passer de l'algèbre élémentaire aux méthodes abstraites de l'algèbre moderne.

Dans les six premiers chapitres l'auteur donne une étude détaillée des déterminants et des systèmes d'équations linéaires, introduit les nombres complexes et les opérations sur les matrices, développe la théorie des polynômes et des formes quadratiques.

Dans les chapitres VII et VIII l'auteur traite les notions primaires de l'algèbre linéaire. Nous voyons dans le chapitre X que l'algèbre linéaire, la théorie des polynômes et des fonctions rationnelles se généralisent au cas d'un champ de base quelconque. C'est à partir de ce chapitre que l'auteur introduit et utilise les méthodes de l'algèbre moderne. Le lecteur y rencontrera les notions très importantes d'anneau et de champs. Ces notions permettent de développer avec une grande généralité la théorie des polynômes de plusieurs indéterminées dont les coefficients sont des éléments d'un champ de base quelconque donné.

Puis on étudie les matrices polynomiales sur un champ de base quelconque qui sont utilisées pour l'élaboration de la théorie des matrices jordaniennes. Le dernier chapitre est consacré à l'étude des groupes; il peut être considéré comme une introduction à la branche importante de l'algèbre moderne, dite « théorie des groupes ».

Les paragraphes marqués par l'astérisque (*) peuvent être sautes en première lecture.

Ce cours d'algèbre supérieure est le manuel de base à l'usage des étudiants de la Faculté de mathématiques de l'Université de Moscou.

Il a eu neuf rééditions et est un des meilleurs cours d'algèbre en Union Soviétique. Nous espérons qu'il trouvera un bon accueil parmi les lecteurs de pays d'expression française. Nous serons reconnaissants à tous ceux qui auront bien voulu contribuer par leurs remarques à l'amélioration de ce livre et, bien entendu, nous en tiendrons compte lors des rééditions ultérieures.

L'éditeur

INTRODUCTION

A la Faculté de mathématiques l'étude commence par trois disciplines de base: l'analyse, la géométrie analytique et l'algèbre supérieure, qui, ayant des points communs, se superposent parfois et constituent les fondements des mathématiques modernes.

L'algèbre supérieure, objet d'étude de notre cours, est une généralisation naturelle du cours d'algèbre élémentaire professé à l'école secondaire, ce dernier étant centré sur la résolution des équations. Cette étude commence par le cas très simple d'une équation du premier degré à une inconnue, puis on considère, d'une part, les systèmes de deux (ou trois) équations du premier degré à deux (ou trois) inconnues et, d'autre part, le cas d'une équation du 2[e] degré à une inconnue et les types particuliers d'équations de degrés supérieurs se ramenant facilement à des équations du 2[e] degré (ex. les équations bicarrées).

Ces deux directions sont encore développées dans le cours d'algèbre supérieure et en constituent deux branches importantes dont la première, les fondements de l'algèbre linéaire, a pour but l'étude des systèmes arbitraires d'équations du premier degré (ou linéaires). Lorsque le nombre des équations est égal à celui des inconnues, on applique pour la résolution de tels systèmes la théorie des déterminants. Cependant, lorsque le nombre des équations ne coïncide pas avec celui des inconnues (situation qui pourrait paraître bizarre du point de vue de l'algèbre élémentaire, mais s'avère très importante pour les applications), la théorie des déterminants fait défaut et l'on est obligé de recourir à celle des matrices, une matrice étant un tableau carré ou rectangulaire de nombres à plusieurs lignes et colonnes. Cette théorie qui s'est révélée très féconde a trouvé de nombreuses applications en dehors de la théorie des systèmes d'équations linéaires. D'autre part, l'étude des systèmes d'équations linéaires a nécessité l'introduction et l'examen des espaces à plusieurs dimensions (espaces vectoriels ou linéaires). Il s'agit d'une notion purement mathématique, ou plutôt algébrique, qui constitue un outil puissant pour la recherche mathématique, physique et mécanique.

La seconde branche du cours d'algèbre supérieure, dite algèbre es polynômes, étudie les équations de degré quelconque à une

inconnue. Puisqu'il existait des formules permettant de résoudre les équations du 2e degré, on en a voulu trouver également pour la résolution des équations de degrés supérieurs. C'était effectivement la direction d'évolution de cette branche de l'algèbre, et les formules correspondantes pour les équations du 3e et du 4e degré ont été trouvées au XVIe siècle. Puis, ce furent des années de vains efforts pour établir des formules donnant les racines des équations du 5e degré et de degrés supérieurs en fonction des coefficients, au moyen de radicaux. Enfin, au début du XIXe siècle on a prouvé que de telles formules n'existent pas et donné des exemples concrets d'équations du 5e degré et de degrés supérieurs à coefficients entiers qu'on ne peut résoudre par radicaux.

Ce phénomène ne doit pas trop nous inquiéter, car déjà dans le cas des équations du 3e et du 4e degré, les formules sont très encombrantes et pratiquement inutilisables. D'autre part, les ingénieurs et les physiciens ont à faire à des équations dont les coefficients sont, en général, des grandeurs obtenues par mesure, c'est-à-dire de grandeurs approchées, de sorte que les racines ne doivent être calculées qu'approximativement, avec une précision donnée. De là résultent toutes sortes de méthodes de résolution approchée des équations, dont le cours d'algèbre supérieure n'étudie que les plus simples.

Cependant, le problème fondamental de l'algèbre des polynômes n'est pas le calcul des racines d'une équation, mais le problème de leur existence. Certaines équations du 2e degré à coefficients réels, on le sait, n'ont pas de racines réelles. Si l'on complète l'ensemble des nombres réels de façon à obtenir l'ensemble des nombres complexes, on constate que les équations du 2e degré possèdent déjà des racines et qu'il en est de même des équations du 3e et du 4e degré puisqu'on connaît les formules explicites qui donnent leurs racines. Il est naturel de se demander s'il existe des équations du 5e degré et de degré plus élevé n'ayant pas de racines, même parmi les nombres complexes. S'il en était ainsi, il conviendrait d'introduire des ensembles encore plus vastes que celui des nombres complexes, afin que les équations en question possèdent des racines. La réponse à cette question est fournie par un théorème très important qui dit que toute équation à coefficients numériques quelconques, réels ou complexes, possède des racines complexes (et éventuellement réelles); en outre, le nombre de celles-ci coïncide avec le degré de l'équation.

Sur ce, nous terminons notre bref exposé du contenu du cours d'algèbre supérieure. Il convient de souligner que l'algèbre supérieure n'est qu'une introduction à la théorie algébrique générale, laquelle, très féconde, présente plusieurs branches et se développe constamment. Nous esquisserons de facon encore plus succincte les

branches algébriques qui se trouvent, pour l'essentiel, en dehors du cours d'algèbre supérieure.

L'algèbre linéaire qui a pour objet essentiel l'étude des matrices et des applications linéaires dans les espaces vectoriels comprend également la théorie des formes, la théorie des invariants et l'algèbre tensorielle, cette dernière très importante pour la géométrie différentielle. Dépassant le cadre de l'algèbre, la théorie des espaces vectoriels s'étend, en analyse, au cas des espaces à une infinité de dimensions. L'algèbre linéaire, grâce à ses nombreuses applications tant en mathématiques qu'en mécanique, physique et technique, détient, par son importance, la première place parmi les autres branches algébriques.

L'algèbre des polynômes étudiant les équations de degré quelconque à une inconnue peut être considérée à présent comme branche achevée. Son développement ultérieur est partiellement lié à celui de la théorie des fonctions d'une variable complexe, mais aboutit surtout à la théorie des champs comprenant l'algèbre des polynômes; nous y reviendrons. L'étude des systèmes d'équations non linéaires de degré quelconque à plusieurs inconnues (c'est un problème extrêmement complexe qui englobe les deux branches du cours d'algèbre supérieure mais dépasse le cadre du présent cours) fait l'objet essentiel d'une théorie mathématique spéciale, dite géométrie algébrique.

Evariste Galois (1811-1832) fut le premier à énoncer les conditions sous lesquelles une équation polynomiale est résoluble par radicaux. Ses recherches déterminèrent de nouvelles orientations en algèbre, ce qui aboutit au XXe siècle, à la suite des travaux d'Emmy Noether (1882-1935), à une nouvelle perspective pour l'algèbre. Il ne fait pas de doute que le problème majeur de l'algèbre moderne n'est plus l'étude des équations, mais celle des opérations algébriques, telles que l'addition et la multiplication, par exemple, opérations portant non plus sur les nombres, mais sur des objets de nature plus générale.

Déjà en physique élémentaire du programme de l'école secondaire, l'on recourt à l'addition de vecteurs représentant les forces. Les disciplines mathématiques professées en première et deuxième années d'Universités et dans les Ecoles Normales abondent en exemples d'opérations algébriques: addition et multiplication de matrices et de fonctions, opérations sur les applications d'espaces, sur les vecteurs, etc. Ces opérations ressemblent en général aux opérations sur les nombres et portent la même dénomination, mais il arrive que certaines propriétés des opérations sur les nombres ne soient pas conservées. Ainsi, très souvent et dans des cas fort importants, les opérations deviennent non commutatives (le produit dépend de l'ordre des facteurs) ou non associatives (le produit de trois facteurs dépend de la place des parenthèses).

Les systèmes algébriques importants, c'est-à-dire des ensembles d'éléments de nature quelconque munis de certaines opérations algébriques, actuellement soumis à l'étude la plus détaillée, sont, par exemple, les champs, systèmes algébriques munis, tout comme l'ensemble des nombres complexes et celui des nombres réels, d'opérations d'addition et de multiplication commutatives, associatives, liées par la loi de distributivité et possédant des opérations inverses, à savoir la soustraction et la division. La théorie des champs s'est trouvée être un terrain propice au développement de la théorie des équations, et ses branches principales que sont la théorie des champs des nombres algébriques et la théorie des champs des fonctions algébriques ont assuré sa liaison respectivement avec la théorie des nombres et celle des fonctions d'une variable complexe. Le cours d'algèbre supérieure comprend une introduction élémentaire à la théorie des champs, certaines de ses parties (polynômes de plusieurs indéterminées, forme normale des matrices) étant exposées pour le cas général d'un champ de base quelconque.

La notion d'anneau est encore plus générale que celle de champ. Elle ne suppose plus la division, et la multiplication peut être non commutative, voire non associative. Citons, comme anneaux, l'ensemble des nombres entiers, celui des polynômes d'une indéterminée et celui des fonctions réelles d'une variable réelle. La théorie des anneaux englobe également certaines vieilles branches (théorie des systèmes hypercomplexes, théorie des idéaux); elle est liée à plusieurs disciplines mathématiques, en particulier à l'analyse fonctionnelle, et, de plus, connaît certaines applications en physique. Le cours d'algèbre supérieure ne contient en fait que la définition d'un anneau.

Le domaine d'application de la théorie des groupes est encore plus vaste. On appelle groupe un système algébrique muni d'une seule opération de base, cette dernière étant associative, mais pas nécessairement commutative, et de l'opération inverse, dite division, si l'opération de base est la multiplication. Tels sont, par exemple, l'ensemble des nombres entiers muni de l'opération d'addition et l'ensemble des nombres réels positifs muni de l'opération de multiplication. La théorie des groupes joue actuellement un rôle immense. Déjà Galois l'avait pour l'essentiel utilisée pour étudier la résolution des équations polynomiales, maintenant elle constitue un outil important qui connaît des applications nombreuses dans la théorie des champs, en géométrie, en topologie et même en dehors des mathématiques: en cristallographie et en physique théorique. Pour l'étendue de ses applications, la théorie des groupes se classe seconde, immédiatement après l'algèbre linéaire. Notre cours consacre un chapitre aux fondements de cette théorie.

Une nouvelle branche de l'algèbre, la théorie des structures, a pris naissance et commencé à se développer, il y a une trentaine d'années. On appelle structure un système algébrique muni de deux opérations, addition et multiplication, qui sont commutatives, associatives et, de plus, telles que: 1) la somme et le produit d'un élément par lui-même redonnent cet élément; 2) pour tout couple d'éléments *a* et *b*, si la somme $a + b$ est égale à l'un d'eux, soit *a*, le produit est égal à l'autre, *b*, et réciproquement. L'ensemble des nombres entiers positifs où l'on introduit comme opérations le calcul du plus grand commun diviseur et du plus petit commun multiple constitue un exemple de structure. On découvre dans la théorie des structures des rapports très intéressants avec les théories des groupes, des anneaux et des ensembles, et il s'est révélé qu'une vieille branche de la géométrie, la géométrie projective, n'était au fond qu'une partie de la théorie des structures; il convient également de mentionner l'application des structures en théorie des circuits électriques.

Le parallélisme qui existe entre diverses parties des théories des groupes, des anneaux et des structures a donné naissance à la théorie générale des systèmes algébriques (ou des algèbres universelles). Celle-ci ne fait que débuter. Néanmoins, les contours de cette nouvelle théorie sont déjà assez nets et ont mis en relief ses rapports avec la logique mathématique, ce qui présage un développement assez rapide de cette science.

Bien entendu, le schéma que nous venons d'ébaucher est loin d'englober tous les aspects de l'algèbre moderne. En particulier, il existe des branches algébriques voisines des autres théories mathématiques. Telle est, par exemple, l'algèbre topologique dont l'objet d'étude est les systèmes algébriques munis des opérations algébriques et d'une topologie (c'est-à-dire d'une notion de limite définie pour les éléments du système), les opérations devant être continues par rapport à la topologie introduite dans le système. La théorie des groupes de Lie, qui est très proche de l'algèbre topologique, trouve de nombreuses applications en géométrie, en physique théorique et en hydrodynamique. Cette théorie des groupes de Lie est le véritable carrefour des méthodes algébriques, topologiques, géométriques et fonctionnelles, de sorte qu'il serait logique de la considérer comme une branche mathématique à part. Il existe également une théorie des systèmes algébriques ordonnés qui est apparue grâce aux recherches portant sur les fondements de la géométrie et a trouvé des applications en analyse fonctionnelle. Enfin, nous sommes témoins des progrès rapides de l'algèbre différentielle, qui établit des rapports nouveaux entre l'algèbre et la théorie des équations différentielles.

Bien sûr, l'essor brillant de l'algèbre n'est pas dû au hasard. Il s'inscrit dans le cadre du développement des mathématiques en

général et est déterminé, pour une large part, par la nécessité de résoudre les problèmes posés à l'algèbre par les autres disciplines mathématiques. D'autre part, l'évolution de l'algèbre a exercé et continue d'exercer sur celle des branches voisines une influence de plus en plus considérable, étant donné son vaste champ d'application: on dit fort justement que les mathématiques modernes « s'algébrisent » de plus en plus.

Les théories algébriques mentionnées ci-dessus sortent pour l'essentiel du cadre du cours d'algèbre supérieure mais notre dessein était de donner au lecteur une vue exacte de la place occupée par l'algèbre supérieure dans la science algébrique et l'ensemble de l'édifice mathématique.

Chapitre I — SYSTÈMES D'ÉQUATIONS LINÉAIRES. DÉTERMINANTS

§ 1. Méthode d'élimination successive des inconnues

Nous commençons ce cours d'algèbre supérieure par l'étude des systèmes d'équations du premier degré à plusieurs inconnues, ou, comme il est admis de les appeler, *équations linéaires* [1].

La théorie des systèmes d'équations linéaires est le point de départ dans l'étude d'une branche importante de l'algèbre, dite « linéaire ». Une grande partie de notre livre, notamment ses trois premiers chapitres, se rapportent à cette théorie. Les coefficients des équations considérées dans ces trois chapitres, les valeurs des inconnues et en général tous les nombres auxquels nous aurons à faire seront supposés réels. D'ailleurs, les résultats de ces chapitres s'étendent automatiquement au cas des nombres complexes, notion que le lecteur connaît du cours d'algèbre de l'école secondaire.

Contrairement à l'algèbre élémentaire, nous allons étudier les systèmes à un nombre quelconque d'équations et d'inconnues; parfois, le nombre d'équations du système ne sera pas égal au nombre d'inconnues. Soit donné un système de s équations à n inconnues. Convenons d'utiliser les symboles suivants: les inconnues seront notées par la lettre x munie inférieurement d'indices : $x_1, x_2, \ldots, x_n$; les équations seront désignées par première, deuxième, ..., $s^{\text{ème}}$ équation; le coefficient de x_j dans la $i^{\text{ème}}$ équation sera noté a_{ij} [2], le second membre de la $i^{\text{ème}}$ équation par b_i.

Avec ces conventions notre système s'écrit sous la forme générale suivante:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{s1}x_1 + a_{s2}x_2 + \ldots + a_{sn}x_n = b_s. \end{array}\right\} \qquad (1)$$

[1] Ce terme est dû à ce qu'en géométrie analytique, une équation du premier degré à deux inconnues représente l'équation d'une droite du plan.

[2] Nous usons donc de deux indices dont le premier désigne le numéro de l'équation, le second celui de l'inconnue. Pour simplifier l'écriture, nous ne séparons pas ces indices par une virgule; ainsi, il n'est pas recommandé, dans le cas de a_{11}, de lire « a indice onze », au lieu de « a indices un, un », ou bien dans le cas de a_{34} « a indice trente-quatre », au lieu de « a indices trois, quatre ».

Les coefficients des inconnues forment un tableau rectangulaire

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{s1} & a_{s2} & \dots & a_{sn} \end{pmatrix}, \qquad (2)$$

qu'on appelle *matrice à s lignes* et *n colonnes*; les nombres a_{ij} sont les *éléments* de la matrice [1]. Si $s = n$ (c'est-à-dire s'il y a autant de lignes que de colonnes), la matrice est alors appelée *matrice carrée d'ordre n*. La diagonale de cette matrice, formée par les éléments $a_{11}, a_{22}, \dots, a_{nn}$, est appelée *diagonale principale*. Une matrice carrée d'ordre n est dite *matrice unité d'ordre n*, si tous les éléments de sa diagonale principale sont égaux à l'unité et si tous les autres éléments, qui n'appartiennent pas à la diagonale principale, sont nuls.

Une suite $k_1, k_2, \dots, k_n$ de n nombres est appelée *solution* du système d'équations linéaires (1) si après substitution des nombres k_i, $i = 1, 2, \dots, n$, aux inconnues x_i toutes les équations de ce système sont vérifiées identiquement [2].

Il peut arriver qu'un système d'équations linéaires n'ait pas de solutions; dans ce cas il est dit *incompatible*. Tel est, par exemple, le système d'équations

$$x_1 + 5x_2 = 1,$$
$$x_1 + 5x_2 = 7,$$

dont les premiers membres sont identiques et les seconds différents. Par conséquent, aucune suite de valeurs des inconnues ne peut satisfaire simultanément à ces deux équations.

Si un système d'équations linéaires a des solutions, il est dit *compatible*. Un système compatible est dit *déterminé* s'il n'a qu'une et seulement une solution (on ne considère que de tels systèmes en algèbre élémentaire). Par contre, ce système est appelé *indéterminé* s'il a plus d'une solution; comme on le verra par la suite, ce système possède une infinité de solutions. Ainsi, le système

$$\left.\begin{aligned} x_1 + 2x_2 &= 7, \\ x_1 + x_2 &= 4 \end{aligned}\right\}$$

est déterminé, car il a la solution $x_1 = 1$, $x_2 = 3$, et comme il est facile de le vérifier par la méthode d'élimination des inconnues, celle-ci est unique. Par contre, le système

---

[1] Considérant la matrice (2) indépendamment du système (1) on voit que le premier indice de l'élément a_{ij} désigne le numéro de la ligne et le second le numéro de la colonne; a_{ij} se trouve donc à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne.

[2] Nous tenons à souligner que la suite $k_1, k_2, \dots, k_n$ de n nombres forme *une* solution du système (1) et non n solutions.

$$\left.\begin{aligned} 3x_1 - x_2 &= 1, \\ 6x_1 - 2x_2 &= 2 \end{aligned}\right\}$$

est indéterminé, car il possède une infinité de solutions

$$x_1 = k, \qquad x_2 = 3k - 1, \tag{3}$$

k étant un paramètre arbitraire ; en outre, les solutions qui s'obtiennent des formules (3) épuisent l'ensemble des solutions du système en question.

Le problème fondamental de la théorie des systèmes d'équations linéaires consiste à élaborer des méthodes permettant de savoir si un système d'équations donné est compatible ou non et, dans le cas de compatibilité, d'établir le nombre de ses solutions, ainsi que de donner un procédé pour trouver toutes les solutions.

Nous commencerons par la méthode la plus commode pour trouver pratiquement les solutions des systèmes à coefficients numériques, à savoir *celle d'élimination successive des inconnues* (ou *méthode de Gauss*).

Faisons d'abord une remarque. Il nous faudra, par la suite, faire les transformations suivantes sur les systèmes d'équations linéaires: multiplier les deux membres d'une des équations du système par un même nombre, puis les retrancher des membres correspondants d'une autre équation du système. Supposons par exemple que les deux membres de la première équation du système (1), multipliés par le nombre c, soient retranchés des membres correspondants de la deuxième équation. Nous obtenons un nouveau système d'équations:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a'_{21}x_1 + a'_{22}x_2 + \ldots + a'_{2n}x_n &= b'_2, \\ a_{31}x_1 + a_{32}x_2 + \ldots + a_{3n}x_n &= b_3, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{s1}x_1 + a_{s2}x_2 + \ldots + a_{sn}x_n &= b_s, \end{aligned}\right\} \tag{4}$$

où

$$a'_{2j} = a_{2j} - ca_{1j} \quad \text{pour} \quad j = 1, 2, \ldots, n, \qquad b'_2 = b_2 - cb_1.$$

Les systèmes d'équations (1) *et* (4) *sont équivalents, c'est-à-dire compatibles ou incompatibles simultanément, et, dans le cas de compatibilité, possèdent les memes solutions.* En effet, soit $k_1, k_2, \ldots, k_n$ une solution du système (1). Evidemment, ces nombres vérifient toutes les équations du système (4), excepté la deuxième. Néanmoins, ils satisfont aussi à la deuxième équation car il suffit de rappeler que cette équation du système (4) s'exprime par la première et la deuxième du système (1). Inversement, toute solution du système (4) vérifie le système (1). En effet, la deuxième équation

du système (1) s'obtient en retranchant des deux membres de la deuxième équation du système (4) les membres correspondants de la première équation de ce système multipliés par le nombre — c.

Il est évident qu'*en appliquant plusieurs fois au système* (1) *les transformations du type décrit ci-dessus, nous obtenons de nouveau un système d'équations équivalent au système initial* (1).

Il est possible que, après avoir fait un certain nombre de transformations de ce genre, nous obtenons une équation dont le premier membre est identiquement nul. Si son second membre l'est aussi, alors elle est satisfaite pour toutes les valeurs des inconnues. *Eliminant cette équation nous sommes conduits à un système équivalent au système initial.* Si, par contre, le second membre de l'équation en question n'est pas nul, il n'existe alors pas de valeurs des inconnues qui vérifient cette équation. Par conséquent, le *système d'équations obtenu ainsi que le système initial, équivalent à ce dernier, sont incompatibles.*

Passons maintenant à la méthode de Gauss.

Soit un système d'équations linéaires (1). Supposons, par exemple, que le coefficient $a_{11} \neq 0$; au cas où il est nul, nous commençons par un autre coefficient non nul de la première équation.

Transformons le système (1) en éliminant l'inconnue x_1 de toutes les équations, sauf la première. Pour cela retranchons les deux membres de la première équation multipliés par le nombre $\frac{a_{21}}{a_{11}}$ des membres correspondants de la deuxième équation. Puis, retranchons les deux membres de la première équation multipliés par $\frac{a_{31}}{a_{11}}$ des membres correspondants de la troisième, etc.

Ce procédé nous conduit à un nouveau système de s équations à n inconnues:

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n &= b_1, \\ a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n &= b'_2, \\ a'_{32}x_2 + a'_{33}x_3 + \ldots + a'_{3n}x_n &= b'_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a'_{s2}x_2 + a'_{s3}x_3 + \ldots + a'_{sn}x_n &= b'_s. \end{aligned}\right\} \qquad (5)$$

Il est inutile de chercher à exprimer explicitement les coefficients a'_{ij} et les seconds membres b'_i par les coefficients et les seconds membres du système initial.

Comme nous le savons, le système d'équations (5) est équivalent au système (1). Transformons à présent le système (5). La première des équations (5) ne devant pas être transformée, nous ne nous occuperons que du sous-système composé de toutes les équations (5), excepté la première. Bien entendu, nous supposons que ce sous-

système ne possède pas d'équations dont les coefficients des premiers membres et les seconds membres seraient identiquement nuls, car nous pouvons toujours les éliminer. Nous supposons également qu'il n'y a pas dans notre sous-système d'équations dont les premiers membres soient identiquement nuls et les seconds membres non nuls, car dans ce cas le système (5) serait incompatible. Il existe donc des coefficients a'_{ij} non nuls. Sans restreindre la généralité on peut supposer que $a'_{22} \neq 0$. Multipliant les deux membres de la deuxième équation respectivement par

$$\frac{a'_{32}}{a'_{22}}, \quad \frac{a'_{42}}{a'_{22}}, \quad \ldots, \quad \frac{a'_{s2}}{a'_{22}}$$

et les retranchant ensuite des deux membres correspondants de toutes les équations du système, à partir de la troisième, nous éliminons l'inconnue x_2 qui ne figure à présent que dans la première et la deuxième des équations. Il vient après ces transformations

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n &= b_1, \\ a'_{22}x_2 + a'_{23}x_3 + \ldots + a'_{2n}x_n &= b'_2, \\ a''_{33}x_3 + \ldots + a''_{3n}x_n &= b''_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a''_{t3}x_3 + \ldots + a''_{tn}x_n &= b''_t \end{aligned}\right\},$$

ce système étant équivalent au système (5) et, par conséquent, au système (1). Il contient à présent t équations, avec $t \leqslant s$, car il est possible que nous ayons éliminé plusieurs équations. Evidemment, le nombre des équations aurait pu diminuer après l'élimination de l'inconnue x_1. Nous devons continuer à transformer toutes les équations, excepté les deux premières.

Quand ce processus d'élimination des inconnues s'arrête-t-il?

Si au cours des transformations nous obtenons une équation dont le premier membre est identiquement nul et le second ne l'est pas, cela signifie, comme on le sait, que le système initial est incompatible.

Dans le cas contraire, nous arrivons au système d'équations suivant (équivalent au système (1)):

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1,k-1}x_{k-1} + a_{1k}x_k + \ldots + a_{1n}x_n &= b_1, \\ a'_{22}x_2 + \ldots + a'_{2,k-1}x_{k-1} + a_{2k}x_k + \ldots + a'_{2n}x_n &= b'_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a^{(k-2)}_{k-1,k-1}x_{k-1} + a^{(k-2)}_{k-1,k}x_k + \ldots + a^{(k-2)}_{k-1,n}x_n &= b^{(k-2)}_{k-1}, \\ a^{(k-1)}_{kk}x_k + \ldots + a^{(k-1)}_{kn}x_n &= b^{(k-1)}_k. \end{aligned}\right\} \quad (6)$$

Ici $a_{11} \neq 0$, $a'_{22} \neq 0$, ..., $a^{(k-2)}_{k-1,k-1} \neq 0$, $a^{(k-1)}_{kk} \neq 0$. Il faut remarquer que $k \leqslant s$ et, bien entendu, $k \leqslant n$.

Dans ce cas le système (1) *est compatible. Il sera déterminé pour* $k = n$ *et indéterminé pour* $k < n$.

En effet, si $k = n$, le système (6) prend la forme

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a'_{22}x_2 + \ldots + a'_{2n}x_n &= b'_2, \\ \ldots\ldots\ \ldots\ldots\ldots & \\ a_{nn}^{(n-1)}x_n &= b_n^{(n-1)}. \end{aligned}\right\} \qquad (7)$$

La dernière équation nous donne une valeur bien déterminée de l'inconnue x_n. En la substituant à x_n dans l'avant-dernière équation, nous obtenons une valeur bien déterminée de l'inconnue x_{n-1}. Procédant ainsi, nous arrivons à la conclusion que le système (7) et par conséquent le système (1) ont tous les deux une solution unique, c'est-à-dire ils sont tous les deux compatibles et déterminés.

Si, par contre, $k < n$, les inconnues « libres » (non principales) $x_{k+1}, \ldots, x_n$ peuvent prendre des valeurs arbitraires; en attribuant aux inconnues $x_{k+1}, \ldots, x_n$ des valeurs quelconques, le procédé employé ci-dessus pour le système (7), mais appliqué cette fois-ci au système (6), permet de trouver les valeurs correspondantes des inconnues $x_1, \ldots, x_k$. Les valeurs des inconnues $x_{k+1}, \ldots, x_n$ pouvant être choisies arbitrairement, le système (6) et, par conséquent, le système (1) possèdent une infinité de solutions. Autrement dit, dans ce cas, les systèmes (6) et (1) sont compatibles, mais indéterminés. Il est facile de vérifier que (en attribuant toutes les valeurs possibles aux inconnues $x_{k+1}, \ldots, x_n$) cette méthode nous donne toutes les solutions du système (1).

On peut supposer qu'un système d'équations linéaires puisse également être réduit par la méthode de Gauss à une forme différente des formes (6) et (7). Notamment, il semble possible de le ramener à un système qui s'obtient en ajoutant à un système du type (7) un certain nombre d'équations où n'intervient que l'inconnue x_n. Quand bien même il en serait ainsi, cela signifierait que les transformations ne sont pas encore achevées. En effet, comme $a_{nn}^{(n-1)} \neq 0$, l'on peut dans ce cas éliminer l'inconnue x_n de toutes les équations à partir de la $(n+1)^{\text{ème}}$.

Il faut remarquer que la forme « triangulaire » du système d'équations (7) ou la forme « trapézoïdale » du système d'équations (6) (pour $k < n$) sont dues à la supposition que les coefficients a_{11}, a'_{22}, etc. ne sont pas nuls. Dans le cas général, le système d'équations auquel nous sommes amenés après l'élimination des inconnues ne prend la forme triangulaire (ou trapézoïdale) qu'après un rénumérotage convenable des inconnues.

Résumant les résultats ci-dessus, nous constatons que *la méthode de Gauss est applicable à tout système d'équations linéaires. En outre,*

le système est incompatible si à la suite de transformations nous obtenons une équation dont le premier membre est identiquement nul et le second ne l'est pas. Si, par contre, au cours de transformations nous n'obtenons pas de telles équations, c'est que notre système est compatible. Il est en même temps déterminé si l'on peut le réduire à la forme triangulaire (7) *et indéterminé s'il se ramène à la forme trapézoïdale* (6) *avec* $k < n$.

Appliquons tout ce qui vient d'être dit à un système *homogène*, c'est-à-dire à un système dont les seconds membres sont nuls. Un tel système est toujours compatible, car il a au moins une solution, à savoir la *solution triviale* (0, 0, . . ., 0). Supposons que notre système homogène ait *plus* d'inconnues que d'équations. Alors, ce système ne peut pas être réduit à la forme triangulaire, car la méthode de Gauss ne peut que diminuer le nombre des équations; par conséquent, ce système se ramène à la forme trapézoïdale, c'est-à-dire il est indéterminé.

Autrement dit, *si un système d'équations linéaires homogènes a plus d'inconnues que d'équations, il possède, outre la solution triviale, d'autres solutions non triviales,* où certaines inconnues (parfois même toutes) sont non nulles. Dans ce cas *le système a une infinité de solutions non triviales.*

Pour résoudre un système d'équations linéaires par la méthode de Gauss, il faut d'abord former la matrice des coefficients, puis y ajouter la colonne des seconds membres. Il est utile de séparer la matrice des coefficients de cette colonne par un trait vertical et faire ensuite toutes les transformations sur la matrice ainsi « élargie ».

Exemples. 1. Résoudre le système

$$\left.\begin{aligned} x_1+2x_2+5x_3&=-9,\\ x_1-x_2+3x_3&=2,\\ 3x_1-6x_2-x_3&=25.\end{aligned}\right\}$$

Transformons la matrice élargie du système :

$$\left(\begin{array}{rrr|r}1&2&5&-9\\1&-1&3&2\\3&-6&-1&25\end{array}\right)\rightarrow\left(\begin{array}{rrr|r}1&2&5&-9\\0&-3&-2&11\\0&-12&-16&52\end{array}\right)\rightarrow\left(\begin{array}{rrr|r}1&2&5&-9\\0&-3&-2&11\\0&0&-8&8\end{array}\right)$$

Ainsi, nous sommes conduits au système

$$\left.\begin{aligned} x_1+2x_2+5x_3&=-9,\\ -3x_2-2x_3&=11,\\ -8x_3&=8,\end{aligned}\right\}$$

qui possède la solution unique

$$x_1=2,\qquad x_2=-3,\qquad x_3=-1.$$

Le système initial est donc determiné.

2. Résoudre le système

$$\left.\begin{aligned} x_1-5x_2-8x_3+x_4&=3,\\ 3x_1+x_2-3x_3-5x_4&=1,\\ x_1\qquad-7x_3+2x_4&=-5,\\ 11x_2+20x_3-9x_4&=2. \end{aligned}\right\}$$

Transformons la matrice élargie du système

$$\left(\begin{array}{rrrr|r} 1 & -5 & -8 & 1 & 3\\ 3 & 1 & -3 & -5 & 1\\ 1 & 0 & -7 & 2 & -5\\ 0 & 11 & 20 & -9 & 2 \end{array}\right)\to\left(\begin{array}{rrrr|r} 1 & -5 & -8 & 1 & 3\\ 0 & 16 & 21 & -8 & -8\\ 0 & 5 & 1 & 1 & -8\\ 0 & 11 & 20 & -9 & 2 \end{array}\right)\to$$

$$\to\left(\begin{array}{rrrr|r} 1 & -5 & -8 & 1 & 3\\ 0 & -89 & 0 & -29 & 160\\ 0 & 5 & 1 & 1 & -8\\ 0 & -89 & 0 & -29 & 162 \end{array}\right)\to\left(\begin{array}{rrrr|r} 1 & -5 & -8 & 1 & 3\\ 0 & -89 & 0 & -29 & 160\\ 0 & 5 & 1 & 1 & -8\\ 0 & 0 & 0 & 0 & 2 \end{array}\right)$$

Nous sommes conduits à un système contenant l'équation $0=2$. Donc, le système initial est incompatible.

3. Résoudre le système

$$\left.\begin{aligned} 4x_1+x_2-3x_3-x_4&=0,\\ 2x_1+3x_2+x_3-5x_4&=0,\\ x_1-2x_2-2x_3+3x_4&=0. \end{aligned}\right\}$$

C'est un système d'équations homogènes. En outre, il possède plus d'inconnues que d'équations; le système doit donc être indéterminé. Les seconds membres étant nuls, nous ne transformons que la matrice des coefficients

$$\begin{pmatrix} 4 & 1 & -3 & -1\\ 2 & 3 & 1 & -5\\ 1 & -2 & -2 & 3 \end{pmatrix}\to\begin{pmatrix} 0 & 9 & 5 & -13\\ 0 & 7 & 5 & -11\\ 1 & -2 & -2 & 3 \end{pmatrix}\to\begin{pmatrix} 0 & 2 & 0 & -2\\ 0 & 7 & 5 & -11\\ 1 & -2 & -2 & 3 \end{pmatrix}$$

Nous sommes conduits au système

$$\left.\begin{aligned} 2x_2\qquad\quad-2x_4&=0,\\ 7x_2+5x_3-11x_4&=0,\\ x_1-2x_2-2x_3+3x_4&=0. \end{aligned}\right\}$$

On peut prendre comme inconnues « libres » (non principales) aussi bien x_2 que x_4. Soit $x_4=\alpha$. La première équation donne alors: $x_2=\alpha$; on déduit ensuite de la deuxième équation $x_3=\frac{4}{5}\alpha$ et, finalement, on obtient de la troisième équation $x_1=\frac{3}{5}\alpha$. Ainsi

$$\frac{3}{5}\alpha,\ \alpha,\ \frac{4}{5}\alpha,\ \alpha$$

est la forme générale des solutions du système donné.

§ 2. Déterminants du deuxième et du troisième ordre

La méthode de résolution des systèmes d'équations linéaires, exposée au paragraphe précédent, est très simple et ne nécessite que des calculs d'un même type facilement réalisables sur les ordinateurs. Néanmoins, son défaut essentiel est de ne pas permettre de formuler au moyen des coefficients et des seconds membres les conditions pour qu'un système donné soit compatible ou déterminé. D'autre part, même dans le cas d'un système déterminé, cette méthode ne permet pas de trouver les formules exprimant la solution du système par ses coefficients et ses seconds membres. Pourtant, tout ceci est nécessaire pour l'étude de certains problèmes théoriques, en particulier, pour la géométrie. C'est pourquoi la théorie des systèmes d'équations linéaires doit être développée par d'autres méthodes plus efficaces. Le cas général sera étudié dans le chapitre suivant, tandis que ce chapitre sera consacré à l'étude des systèmes déterminés qui ont autant d'équations que d'inconnues. Nous commencerons par les systèmes à deux et trois inconnues étudiés dans le cours d'algèbre élémentaire.

Soit un *système de deux équations linéaires à deux inconnues*

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1, \\ a_{21}x_1 + a_{22}x_2 &= b_2, \end{aligned}\right\} \tag{1}$$

dont les coefficients forment une matrice carrée du deuxième ordre

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}. \tag{2}$$

Appliquant la méthode d'identification des coefficients au système (1), il vient

$$(a_{11}a_{22} - a_{12}a_{21})\, x_1 = b_1a_{22} - a_{12}b_2,$$
$$(a_{11}a_{22} - a_{12}a_{21})\, x_2 = a_{11}b_2 - b_1a_{21}.$$

Supposons que $a_{11}a_{22} - a_{12}a_{21} \neq 0$. Alors

$$x_1 = \frac{b_1a_{22} - a_{12}b_2}{a_{11}a_{22} - a_{12}a_{21}}, \qquad x_2 = \frac{a_{11}b_2 - b_1a_{21}}{a_{11}a_{22} - a_{12}a_{21}}. \tag{3}$$

Substituant dans les équations (1) les valeurs trouvées aux inconnues correspondantes il est facile de vérifier que (3) est une solution du système (1); le problème d'unicité de la solution sera étudié au § 7.

Le dénominateur commun dans les formules (3) s'exprime de façon très simple par les éléments de la matrice (2): il est égal au produit des éléments de la diagonale principale duquel on retranche le produit des éléments de la diagonale non principale. Ce nombre est appelé *déterminant* de la matrice (2), ou encore *déterminant*

du deuxième ordre, car la matrice (2) est une matrice du deuxième ordre. Pour désigner le déterminant de la matrice (2), nous utiliserons le symbole suivant: on écrit la matrice (2) en mettant à la place de chaque parenthèse un trait vertical; ainsi,

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}. \tag{4}$$

Exemples.

1) $$\begin{vmatrix} 3 & 7 \\ 1 & 4 \end{vmatrix} = 3\cdot 4 - 7\cdot 1 = 5\ ;$$

2) $$\begin{vmatrix} 1 & -2 \\ 3 & 5 \end{vmatrix} = 1\cdot 5 - (-2)\cdot 3 = 11.$$

Il faut souligner, une fois de plus, que le déterminant d'une matrice est un nombre, tandis que la matrice carrée à laquelle ce nombre est associé est un tableau de nombres. Les produits $a_{11}a_{22}$ et $a_{12}a_{21}$ sont appelés *termes* d'un déterminant du deuxième ordre.

Les numérateurs des expressions (3) ont la même forme que leur dénominateur, c'est-à-dire ils sont aussi des déterminants du deuxième ordre. Le numérateur de l'expression donnant x_1 n'est autre que le déterminant de la matrice qui s'obtient de la matrice (2) par substitution de la colonne des seconds membres du système (1) à la première colonne de la matrice (2); de même, le numérateur de l'expression donnant x_2 est le déterminant de la matrice qui s'obtient de la matrice (2) par substitution de la colonne des seconds membres du système (1) à la deuxième colonne de la matrice (2). Maintenant on peut récrire les formules (3) sous la forme:

$$x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, \qquad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}. \tag{5}$$

Ces formules (dites *formules de Cramer*), donnant la solution d'un système de deux équations à deux inconnues, peuvent s'énoncer de la manière suivante:

Si le déterminant (4), *formé par les coefficients du système d'équations* (1), *n'est pas nul, la solution du système* (1) *s'obtient en prenant pour valeurs des inconnues les fractions dont les dénominateurs sont le déterminant* (4) *et le numérateur de l'inconnue* x_i ($i = 1,2$) *est le déterminant qui s'obtient en substituant à la* $i^{\text{ème}}$ *colonne du déterminant* (4) [1] *la colonne des seconds membres du système* (1).

[1] Pour ne pas alourdir l'exposé nous parlons ici de substitution des colonnes « d'un déterminant ». De même, dans ce qui suit et quand cela sera nécessaire, nous aurons recours aux vocables: lignes, colonnes, éléments, diagonales d'un déterminant, etc.

Exemple. Résoudre le système

$$\left.\begin{aligned} 2x_1 + x_2 &= 7, \\ x_1 - 3x_2 &= -2. \end{aligned}\right\}$$

Le déterminant des coefficients

$$d = \begin{vmatrix} 2 & 1 \\ 1 & -3 \end{vmatrix} = -7$$

n'étant pas nul, nous pouvons appliquer à ce système les formules de Cramer. Les numérateurs dans les expressions des inconnues sont respectivement

$$d_1 = \begin{vmatrix} 7 & 1 \\ -2 & -3 \end{vmatrix} = -19, \qquad d_2 = \begin{vmatrix} 2 & 7 \\ 1 & -2 \end{vmatrix} = -11.$$

Le couple de nombres (valeurs des inconnues x_1 et x_2)

$$x_1 = \frac{d_1}{d} = \frac{19}{7}, \qquad x_2 = \frac{d_2}{d} = \frac{11}{7}$$

est donc la solution de notre système.

L'introduction des déterminants du deuxième ordre n'apporte guère de simplifications à la résolution des systèmes de deux équations linéaires à deux inconnues. Du reste, la résolution de ces systèmes sans avoir recours aux déterminants ne comporte aucune difficulté. Il n'en est plus ainsi pour les *systèmes de trois équations linéaires à trois inconnues* où l'introduction des déterminants est déjà plus efficace. Soit un système

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= b_1, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= b_2, \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= b_3, \end{aligned}\right\} \tag{6}$$

dont la matrice des coefficients est

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \tag{7}$$

En multipliant les deux membres de la première équation par le nombre $a_{22}a_{33} - a_{23}a_{32}$, les deux membres de la deuxième par $a_{13}a_{32} - a_{12}a_{33}$, les deux membres de la troisième par $a_{12}a_{23} - a_{13}a_{22}$ et les additionnant, il est facile de vérifier que les coefficients de x_2 et de x_3 s'annulent, c'est-à-dire les inconnues x_2 et x_3 disparaissent, et l'on obtient

$$\begin{aligned} (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - \\ - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32})\, x_1 = b_1a_{22}a_{33} + a_{12}a_{23}b_3 + \\ + a_{13}b_2a_{32} - a_{13}a_{22}b_3 - a_{12}b_2a_{33} - b_1a_{23}a_{32}. \end{aligned} \tag{8}$$

Le coefficient de x_1 dans (8) est appelé *déterminant du troisième ordre*, associé à la matrice (7). On utilise, pour le noter, le même symbole que pour le déterminant du deuxième ordre ; ainsi

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \quad (9)$$

Bien que l'expression (9) d'un déterminant du troisième ordre soit assez encombrante, la loi selon laquelle ses termes sont formés

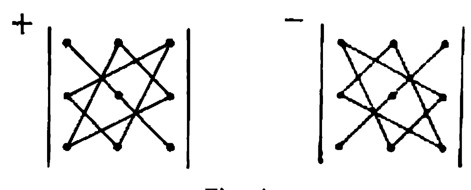


Fig. 1

à partir des éléments de la matrice (7) est très simple. En effet, l'un des trois termes précédés du signe + dans (9) n'est autre que le produit des éléments de la diagonale principale, les deux autres termes étant les produits des éléments des diagonales parallèles à la principale par les éléments situés dans les points les plus éloignés des diagonales correspondantes. Les termes précédés du signe — dans (9) sont formés d'après la même loi appliquée à la diagonale non principale. Nous avons ainsi un procédé permettant de calculer assez rapidement les déterminants du troisième ordre. On a représenté schématiquement sur la figure 1 la règle de calcul des termes précédés du signe + (à gauche) et des termes précédés du signe — (à droite).

Exemples.

1)
$$\begin{vmatrix} 2 & 1 & 2 \\ -4 & 3 & 1 \\ 2 & 3 & 5 \end{vmatrix} = 2\cdot3\cdot5+1\cdot1\cdot2+2\cdot(-4)\cdot3-2\cdot3\cdot2-1\cdot(-4)\cdot5-2\cdot1\cdot3 = 30+2-24-12+20-6 = 10.$$

2)
$$\begin{vmatrix} 1 & 0 & -5 \\ -2 & 3 & 2 \\ 1 & -2 & 0 \end{vmatrix} = 1\cdot3\cdot0+0\cdot2\cdot1+(-5)\cdot(-2)\cdot(-2)-(-5)\cdot3\cdot1-0\cdot(-2)\cdot0-1\cdot2\cdot(-2) = -20+15+4=-1.$$

Le second membre de l'expression (8) est également un déterminant du troisième ordre associé à la matrice qui s'obtient de la matrice (7) par substitution de la colonne des seconds membres du système (6) à sa première colonne. Notons par d le déterminant (9) et par d_j le déterminant qui s'obtient par substitution de la colonne des seconds membres du système (6) à la $j^{\text{ème}}$ colonne du déterminant (9) ($j = 1, 2, 3$). La formule (8) prend alors la forme $dx_1 = d_1$, d'où il vient (à condition que $d \neq 0$)

$$x_1 = \frac{d_1}{d}. \tag{10}$$

Multipliant les équations (6) respectivement par $a_{23}a_{31} - a_{21}a_{33}$, $a_{11}a_{33} - a_{13}a_{31}$, $a_{13}a_{21} - a_{11}a_{23}$, nous obtenons de la même manière pour x_2 l'expression suivante (en supposant toujours $d \neq 0$):

$$x_2 = \frac{d_2}{d}. \tag{11}$$

Enfin, multipliant ces équations respectivement par $a_{21}a_{32} - a_{22}a_{31}$, $a_{12}a_{31} - a_{11}a_{32}$, $a_{11}a_{22} - a_{12}a_{21}$, nous sommes conduits à l'expression suivante pour x_3:

$$x_3 = \frac{d_3}{d}. \tag{12}$$

Substituant aux inconnues x_1, x_2, x_3 dans les équations (6) les valeurs (10) — (12) (les déterminants d et d_j étant développés) on peut vérifier, en faisant des calculs quelque peu laborieux, que toutes les équations (6) sont satisfaites, c'est-à-dire que les nombres (10) — (12) forment une solution du système (6). Ainsi, si le *déterminant des coefficients d'un système de trois équations linéaires à trois inconnues n'est pas nul, la solution de ce système est donnée par les formules de Cramer, qui s'énoncent de la même manière que dans le cas d'un système de deux équations.* Une autre démonstration de cette proposition (qui ne sera pas basée sur les calculs omis ci-dessus) ainsi que la démonstration de l'unicité de la solution (10) — (12) du système (6) seront données au § 7.

Exemple. Résoudre le système:

$$\left.\begin{aligned} 2x_1 - x_2 + x_3 &= 0, \\ 3x_1 + 2x_2 - 5x_3 &= 1, \\ x_1 + 3x_2 - 2x_3 &= 4. \end{aligned}\right\}$$

Le déterminant des coefficients

$$d = \begin{vmatrix} 2 & -1 & 1 \\ 3 & 2 & -5 \\ 1 & 3 & -2 \end{vmatrix} = 28$$

n'étant pas nul, nous pouvons appliquer à ce système les formules de Cramer. Les numérateurs dans les expressions des inconnues étant

$$d_1=\begin{vmatrix} 0 & -1 & 1 \\ 1 & 2 & -5 \\ 4 & 3 & -2 \end{vmatrix}=13, \qquad d_2=\begin{vmatrix} 2 & 0 & 1 \\ 3 & 1 & -5 \\ 1 & 4 & -2 \end{vmatrix}=47, \qquad d_3=\begin{vmatrix} 2 & -1 & 0 \\ 3 & 2 & 1 \\ 1 & 3 & 4 \end{vmatrix}=21,$$

la solution du système est

$$x_1=\frac{13}{28}, \qquad x_2=\frac{47}{28}, \qquad x_3=\frac{21}{28}=\frac{3}{4}.$$

§ 3. Permutations et substitutions

Pour définir et étudier les déterminants d'ordre n, il faut introduire certaines notions et établir certaines propriétés des ensembles finis. Soit M un ensemble fini composé de n éléments. Vu que les éléments de M peuvent être numérotés au moyen des entiers $1, 2, \ldots, n$ et que, en l'occurrence, les propriétés individuelles de ces éléments ne jouent aucun rôle, nous pouvons supposer que les éléments de l'ensemble M sont précisément les entiers $1, 2, \ldots, n$.

L'ordre naturel des n premiers nombres entiers $1, 2, \ldots, n$ n'étant pas le seul possible, nous pouvons les ordonner de plusieurs manières différentes. Ainsi, les nombres 1, 2, 3, 4 peuvent être ordonnés comme suit: 3, 1, 2, 4 ou bien 2, 4, 1, 3, etc. Toute suite des nombres $1, 2, \ldots, n$ ordonnée selon une loi bien déterminée s'appelle *permutation* de n nombres (ou de n éléments).

Le nombre des permutations distinctes de n éléments est égal au produit $1\cdot 2\cdot \ldots \cdot n$, que nous notons par $n!$ (il faut lire factorielle n). En effet, toute permutation est de la forme $i_1, i_2, \ldots, i_n$, la suite $i_1, \ldots, i_n$ étant composée de n nombres distincts prenant les valeurs: $1, 2, \ldots, n$. Par conséquent, i_1 peut prendre a priori n valeurs distinctes $1, 2, \ldots, n$, ce qui donne n permutations différentes. Une fois i_1 fixé, i_2 ne peut prendre que $n-1$ valeurs distinctes, c'est-à-dire il y a $n(n-1)$ facons distinctes de choisir les éléments i_1 et i_2, etc.

Ainsi, pour $n=2$ le nombre des permutations est $2!=2$. Ce sont les permutations 12 et 21 (nous ne séparons pas les éléments par une virgule dans tous les exemples où $n\leqslant 9$); pour $n=3$ ce nombre est $3!=6$, pour $n=4$, il est $4!=24$. Lorsque n croît, le nombre des permutations croît bien plus rapidement; ainsi, pour $n=5$, ce nombre est: $5!=120$, et pour $n=10$, il est déjà égal à 3 628 800.

Echangeant deux éléments distincts d'une permutation (pas forcément ceux qui sont voisins) et laissant tous les autres éléments invariants, nous obtenons, évidemment, une autre permutation. Cette transformation est dite *transposition*.

On peut ordonner les $n!$ permutations de n éléments en une suite de manière que toute permutation s'obtienne par une transposition de celle qui la précède; *en outre la suite peut commencer par une permutation quelconque.*

Il est clair que cette proposition est vraie pour $n = 2$. En effet, si nous commençons par la permutation 12, alors l'ordre cherché est 12, 21 ; si, par contre, nous voulons commencer par 21, l'ordre en question sera 21, 12. Supposons que notre proposition soit prouvée pour $n - 1$. Prouvons-la pour n. Supposons que l'on commence par la permutation

$$i_1, i_2, \ldots, i_n. \tag{1}$$

En vertu de l'hypothèse de récurrence nous pouvons ordonner les permutations de $n - 1$ éléments, conformément à l'énoncé du théorème, en commençant par une permutation quelconque, en particulier, par $i_2, \ldots, i_n$, de telle sorte que les permutations de n éléments qui commencent par i_1 seront ordonnées, selon l'énoncé du théorème, en partant de la permutation (1). Dans la dernière des permutations de n éléments ainsi obtenues, transposons l'élément i_1 avec un autre élément quelconque, par exemple, i_2. Commençant par cette permutation, ordonnons d'après la loi précédente les permutations dont le premier élément est i_2, etc. Il est clair que de cette manière nous obtenons toutes les permutations de n éléments.

Il résulte du théorème démontré ci-dessus qu'*on peut passer d'une permutation donnée à toute autre par une série de transpositions.*

On dit qu'un couple de nombres i, j présente une *inversion* dans une permutation donnée si i précède j et $i > j$. Une permutation est dite *paire* si le nombre d'inversions dans cette permutation est pair et *impaire* dans le cas contraire. Ainsi, la permutation $1, 2, \ldots, n$ est paire quel que soit n, car le nombre d'inversions est égal à zéro. La permutation 451362 ($n = 6$), ayant 8 inversions, est paire. La permutation 38524671 ($n = 8$) est impaire, car elle possède 15 inversions.

Toute transposition change la parité d'une permutation. Pour prouver cette proposition importante, nous allons d'abord considérer le cas où les éléments i et j qu'on transpose sont voisins, c'est-à-dire le cas où la permutation est de la forme $\ldots, i, j, \ldots$, les points de suspension désignant les éléments qui ne changent pas par la transposition. Après cette transposition notre permutation devient $\ldots, j, i, \ldots$. Il est clair que les nombres des inversions présentées par les couples de ces deux permutations, excepté les couples (i, j) et (j, i), coïncident. Si le couple (i, j) ne présente pas d'inversion, en échangeant i et j, le nombre des inversions de la permutation $\ldots, j, i, \ldots$ augmentera d'une unité. Si, par contre, le couple (i, j)

présente une inversion, transposant i et j, le nombre des inversions de la permutation $\ldots, j, i, \ldots$ diminuera d'une unité. Dans les deux cas la parité de la permutation sera changée.

A présent, supposons qu'il y ait s éléments situés entre les éléments qu'on transpose, $s > 0$, c'est-à-dire que la permutation soit de la forme

$$\ldots, i, k_1, k_2, \ldots, k_s, j, \ldots \qquad (2)$$

On peut réaliser la transposition échangeant les éléments i et j par application successive de $2s + 1$ transpositions ne portant que sur des éléments voisins. Notamment, ce sont les transpositions échangeant les éléments k_1 et i, puis k_2 et i, etc. et, enfin, k_s et i; après ces s transpositions vient celle qui permute i et j, puis viennent les transpositions, au nombre de s, échangeant j avec tous les k; finalement i prend la place de j, j prend celle de i, tandis que les éléments k reprennent leurs places initiales. La parité de la permutation ayant changé un nombre impair de fois, les permutations (2) et

$$\ldots, j, k_1, k_2, \ldots, k_s, i, \ldots \qquad (3)$$

sont de parité opposée.

Le nombre des permutations paires de n éléments est égal au nombre des permutations impaires, par conséquent, ce nombre est $\frac{1}{2} n!$ $(n \geqslant 2)$.

En effet, le théorème démontré ci-dessus nous permet d'ordonner les permutations de n éléments de manière que chaque permutation soit une transposition de la précédente. Cet ordre étant, deux permutations voisines sont de parité opposée, autrement dit les permutations paires et impaires alternent. Le nombre $n!$ étant pair pour $n \geqslant 2$, notre proposition en résulte immédiatement.

Introduisons maintenant une autre notion, celle de *substitution de degré n*. Ecrivons deux permutations de n éléments l'une au-dessous de l'autre en les mettant entre parenthèses. Par exemple, pour $n = 5$:

$$\begin{pmatrix} 3 & 5 & 1 & 4 & 2 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}. \qquad (4)$$

Ici [1] le nombre 5 se trouve en dessous du nombre 3, le nombre 2 en dessous du 5, etc. Nous dirons que le nombre 3 *se transforme* en 5, le nombre 5 en 2, le nombre 1 en 3, le nombre 4 en 4 (ou *ne change pas de place*) et, enfin, le nombre 2 en 1. Ainsi, deux permutations écrites sous la forme (4) définissent une application bijective de

[1] Bien qu'il ressemble à une matrice à deux lignes et cinq colonnes, ce signe a un sens tout différent.

l'ensemble, composé des nombres entiers 1, 2, 3, 4, 5, sur lui-même, c'est-à-dire une application qui fait correspondre à chacun de ces nombres un autre nombre de cet ensemble; de plus, à deux nombres distincts correspondent deux nombres distincts. Cet ensemble étant composé de cinq éléments, c'est-à-dire étant un ensemble fini, *chacun* de ces cinq nombres correspond à un des nombres 1, 2, 3, 4, 5, notamment à celui dont il est l'image par l'application envisagée.

Il est clair que l'application bijective (4) peut être donnée au moyen d'autres couples de permutations de cinq éléments écrites l'une en dessous de l'autre. Chacun de ces couples de permutations s'obtient de (4) par un certain nombre de transpositions de colonnes.

Telles sont, par exemple, les substitutions de degré 5:

$$\begin{pmatrix} 2 & 1 & 5 & 3 & 4 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 5 & 2 & 4 & 3 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 2 & 5 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}. \tag{5}$$

Ici 3 se transforme toujours en 5, 5 en 2, etc.

De même, deux permutations de n éléments, écrites l'une en dessous de l'autre, définissent une application bijective de l'ensemble des n nombres entiers $1, 2, \ldots, n$ sur lui-même. Toute application bijective A de l'ensemble des entiers $1, 2, \ldots, n$ sur lui-même est appelée *substitution de degré n*. Evidemment, toute substitution A de degré n peut être exprimée au moyen de deux permutations, écrites l'une en dessous de l'autre, soit

$$A = \begin{pmatrix} i_1, & i_2, & \ldots, & i_n \\ \alpha_{i_1}, & \alpha_{i_2}, & \ldots, & \alpha_{i_n} \end{pmatrix}, \tag{6}$$

α_i étant le nombre que la substitution A fait correspondre au nombre i, $i = 1, 2, \ldots, n$.

Toute substitution A de degré n possède une multitude d'écritures de la forme (6). Ainsi, (4) et (5) sont des formes différentes d'une même substitution de degré 5.

On peut passer de l'une des formes (6) d'une substitution A à une autre par un certain nombre de transpositions de colonnes. En outre, procédant de la sorte, on peut toujours obtenir pour toute substitution A une forme (6) telle que la première (ou bien la deuxième) ligne soit une permutation donnée de n éléments. En particulier, toute substitution A de degré n peut être mise sous la forme

$$A = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}, \tag{7}$$

c'est-à-dire sous la forme où la première ligne est la permutation identique. Il découle de la forme (7) que deux substitutions de degré

n se distinguent l'une de l'autre par les permutations dans leurs secondes lignes. Par conséquent, *le nombre de substitutions de degré n est égal à celui de permutations de n éléments*, *c'est-à-dire à* $n!$.[1]

La substitution identique

$$E = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

est un exemple de substitution de degré n, elle conserve à la même place tous les éléments.

Il faut remarquer que le rôle joué par les deux lignes d'une substitution A (6) n'est pas le même. Transposant les lignes nous obtenons, en général, une autre substitution. Par exemple, les substitutions de degré 4

$$\begin{pmatrix} 2 & 1 & 4 & 3 \\ 4 & 3 & 1 & 2 \end{pmatrix} \text{ et } \begin{pmatrix} 4 & 3 & 1 & 2 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

sont distinctes, car au nombre 2 la première fait correspondre le nombre 4 et la seconde le nombre 3.

Ecrivons une substitution A de degré n sous une forme quelconque. Les permutations formant respectivement la première et la seconde ligne de A peuvent avoir la même parité ou être de parité opposée. On sait qu'on peut passer de l'une des formes d'une substitution A à une autre, en appliquant un certain nombre de transpositions à la ligne supérieure et celles correspondantes à la ligne inférieure. Bien entendu, effectuant une transposition dans la ligne supérieure de (6) et la transposition correspondante dans la ligne inférieure, nous changeons simultanément la parité des deux permutations formant la substitution A. Par conséquent, ayant au début la même parité (ou bien la parité opposée), les deux permutations conservent cette propriété après les transpositions. Il en découle que *deux permutations formant une substitution de degré n sont de même parité ou de parité opposée*, *indépendamment de la forme sous laquelle la substitution est écrite*. Une substitution A est appelée *paire*, si les permutations qui la forment sont de même parité; elle est dite *impaire* dans le cas contraire. En particulier, la substitution identique est paire.

Utilisant la forme (7) des substitutions, c'est-à-dire la forme où la première ligne est la permutation paire $1, 2, \dots, n$, on voit que la parité d'une substitution A est définie par la parité de la

---

[1] Ces dernières considérations montrent qu'il n'y a aucune différence entre les notions de permutation de n éléments et de substitution de degré n. Dans la littérature mathématique française on use généralement du terme « permutation » mais on rencontre parfois des auteurs qui emploient le terme « substitution ». Nous conservons ici le style de l'auteur. (*N.d.T.*)

permutation $\alpha_1, \alpha_2, \ldots, \alpha_n$, constituant sa seconde ligne. Il en résulte que le *nombre de substitutions paires de degré n est égal à celui de substitutions impaires, c'est-à-dire à* $\frac{1}{2} n!$.

On peut aussi définir la parité d'une substitution de degré n de manière suivante. Si dans (6) la parité des deux lignes est la même, alors le nombre des inversions dans ces deux lignes est simultanément pair ou impair, de sorte que dans ce cas le nombre total des inversions est toujours pair ; si, par contre, la parité des lignes dans (6) est opposée, alors le nombre total des inversions dans les deux lignes est impair. Ainsi, *une substitution A de degré n, écrite sous une forme quelconque, est dite paire si le nombre total des inversions dans ses deux lignes est pair et impaire dans le cas contraire.*

Exemple. Soit la substitution de degré 5

$$\begin{pmatrix} 3 & 1 & 4 & 5 & 2 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

La première ligne contient 4 inversions, la seconde en a 7. Le nombre total des inversions étant 11, la substitution en question est impaire.

Mettons cette substitution sous la forme

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}.$$

Le nombre des inversions dans sa première ligne étant nul et dans la seconde 5, le nombre total est impair. On voit que les différentes formes d'une même substitution ont le nombre d'inversions différent, mais chaque fois le nombre total des inversions a la même parité.

A présent, nous allons donner d'autres définitions de la parité des substitutions de degré n équivalentes aux définitions précédentes[1]. Définissons d'abord la *multiplication des substitutions* de degré n, qui est d'ailleurs d'un grand intérêt par elle-même. On sait qu'une substitution de degré n est une application bijective de l'ensemble $1, 2, \ldots, n$ sur lui-même. Deux applications bijectives de l'ensemble $1, 2, \ldots, n$ sur lui-même, accomplies dans un ordre bien déterminé, définissent manifestement une troisième application bijective de cet ensemble sur lui-même. Autrement dit, deux substitutions appliquées l'une après l'autre nous conduisent à une troisième substitution également bien définie, dite *produit* des substitutions données. Par exemple, le produit des substitutions de degré 4

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

[1] Nous n'aurons besoin de ces définitions qu'au chapitre XIV, de sorte qu'elles peuvent être omises en première lecture.

est la substitution

$$AB=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}.$$

En effet, la substitution A transforme l'élément 1 en l'élément 3 et la substitution B transforme l'élément 3 en l'élément 4; par conséquent, AB transforme l'élément 1 en l'élément 4, etc.

On ne peut multiplier que les substitutions de même degré. *La multiplication des substitutions de degré n n'est pas commutative pour $n \geqslant 3$.* En effet, pour les substitutions précédentes A et B, le produit BA est de la forme

$$BA=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{pmatrix},$$

c'est-à-dire la substitution BA ne coïncide pas avec la substitution AB. On peut donner des exemples de non-commutativité pour tout n, $n \geqslant 3$, bien qu'il arrive parfois que certains couples de substitutions commutent.

La multiplication des substitutions de degré n est associative, c'est-à-dire on peut parler du produit d'un nombre fini, quelconque, de substitutions, l'ordre des facteurs dans ce produit devant être bien déterminé (rappelons que la multiplication n'est pas commutative). En effet, soient A, B, C trois substitutions de degré n; supposons que l'image de l'élément i_1, $1 \leqslant i_1 \leqslant n$, par la substitution A soit l'élément i_2, l'image de i_2 par B soit i_3 et celle de i_3 par C soit i_4. Alors, la substitution AB transforme i_1 en i_3, et la substitution BC i_2 en i_4. Ainsi, $(AB)\,C$ et $A\,(BC)$ transforment i_1 en i_4. Il est clair que le *produit d'une substitution A de degré n par la substitution identique E, ainsi que le produit de E par A, donne toujours la substitution A*:

$$AE=EA=A.$$

Enfin, nous appelons substitution *inverse* de A une substitution de degré n, notée A^{-1}, telle que

$$AA^{-1}=A^{-1}A=E.$$

Il est facile de vérifier qu'une substitution

$$A=\begin{pmatrix}1 & 2 & \dots & n\\ \alpha_1 & \alpha_2 & \dots & \alpha_n\end{pmatrix}$$

a pour inverse la substitution

$$A^{-1}=\begin{pmatrix}\alpha_1 & \alpha_2 & \dots & \alpha_n\\ 1 & 2 & \dots & n\end{pmatrix}.$$

A^{-1} s'obtient en intervertissant l'ordre des lignes de A.

Considérons à présent les substitutions de degré n d'un type spécial, à savoir celles qui s'obtiennent de la substitution identique en transposant deux éléments dans sa seconde ligne. Ces substitutions, qui sont manifestement impaires, s'appellent *transpositions* et sont de la forme

$$\begin{pmatrix} \ldots i \ldots j \ldots \\ \ldots j \ldots i \ldots \end{pmatrix}, \tag{8}$$

les points de suspension désignent les éléments qui ne changent pas de place. Convenons de noter cette transposition par le symbole (i, j). La transposition des éléments i et j dans la seconde ligne d'une substitution A écrite sous forme (7) est équivalente à la multiplication à droite de A par la substitution (8), c'est-à-dire à la multiplication de A par (i, j). Comme on le sait, toute permutation de n éléments s'obtient d'une permutation fixée, par exemple, de $(1, 2, \ldots, n)$ en y effectuant successivement un certain nombre de transpositions; ainsi, toute permutation peut être obtenue de la permutation identique au moyen de transpositions dans sa seconde ligne, c'est-à-dire toute substitution de degré n est le produit de la substitution identique par certaines substitutions du type (8). Autrement dit, on peut affirmer que *toute substitution est représentable sous la forme de produit de transpositions* (le facteur E pouvant être omis).

Il existe une multitude de façons de décomposer une substitution donnée en un produit de transpositions. Par exemple, nous pouvons toujours ajouter deux facteurs (i, j) (i, j), dont le produit est égal à E. Voici un exemple moins trivial:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (12)(15)(34) = (14)(24)(45)(34)(13).$$

Une autre définition de la parité des substitutions est basée sur le théorème suivant:

Quelle que soit la décomposition d'une substitution en un produit de transpositions, la parité du nombre de ces transpositions est la même et elle coïncide avec celle de la substitution considérée.

Ainsi, la substitution de l'exemple précédent est impaire, comme il est facile de le vérifier en calculant le nombre des inversions.

Le théorème sera prouvé si nous montrons que le *produit de k transpositions quelconques est une substitution dont la parité est celle du nombre k*. Ceci est manifestement vrai pour $k = 1$, car une transposition est une substitution impaire. Supposons que le théorème soit prouvé pour $(k - 1)$ facteurs. Les nombres $(k - 1)$ et k étant de parité opposée et la multiplication d'une substitution (ici c'est la substitution A_1 composée des $(k - 1)$ premiers facteurs) par une

transposition étant équivalente à l'application de cette transposition dans la seconde ligne de A_1, le théorème est prouvé par la récurrence sur k.

Un moyen commode d'écrire les substitutions, qui permet de trouver facilement leur parité, est la *décomposition des substitutions en cycles*. Une substitution de degré n peut conserver à la même place certains éléments de l'ensemble $1, 2, \ldots, n$, tandis qu'à tout autre elle fait correspondre un élément distinct de ce dernier. On appelle *substitution cyclique*, ou *cycle*, toute substitution qui par sa réitération un nombre suffisant de fois peut pour tout couple d'éléments non conservés faire correspondre l'un de ceux-ci à l'autre. Telle est, par exemple, la substitution de degré 8 :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 6 & 4 & 5 & 2 & 7 & 3 \end{pmatrix},$$

qui échange les entiers 2, 3, 6 et 8 ; en outre, elle fait correspondre l'entier 8 à l'entier 2, 3 à 8, 6 à 3 et 2 à 6.

Toute transposition est un cycle. Par analogie avec les transpositions on a recours à l'écriture suivante, pour désigner les cycles : soit un cycle, on ordonne les éléments qui ne sont pas conservés par ce cycle et on les met entre parenthèses, l'ordre des éléments non conservés étant conforme à celui de leur apparition à la suite de la réitération du cycle considéré ; le premier signe du cycle peut être pris arbitrairement parmi les éléments non conservés par lui ; en outre, le cycle fait correspondre le premier élément au dernier élément de la ligne. Ainsi, pour le cycle ci-dessus l'écriture en question est de la forme :

$$(2\ \ 8\ \ 3\ \ 6).$$

Le nombre des éléments non conservés par un cycle est appelé *longueur* du cycle.

Deux cycles de degré n sont dits *indépendants*, s'ils n'ont pas d'éléments communs non conservés. Il est clair que le produit de deux cycles indépendants ne dépend pas de l'ordre des facteurs.

Toute substitution peut être décomposée d'une façon unique en un produit de cycles indépendants deux à deux. La démonstration de cette proposition ne représente aucune difficulté et peut être omise. En pratique, la décomposition se fait de la manière suivante : on commence par un élément non conservé quelconque et l'on écrit successivement les éléments, images correspondantes du premier élément par la substitution en question réitérée, jusqu'à ce que l'on retrouve le premier élément ; ceci étant, on fixe un élément non conservé quelconque parmi ceux qui n'appartiennent pas au premier cycle, l'élément fixé engendrant par ce même procédé le second cycle, etc.

Exemples.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = (13)\,(254).$$

2) $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 8 & 7 & 6 & 1 & 4 & 3 \end{pmatrix} = (156)\,(38)\,(47).$$

Inversement, pour toute substitution mise sous la forme d'un produit de cycles indépendants, on peut trouver son écriture usuelle (à condition que l'on connaisse le degré de la substitution). Par exemple,

3) $$(1372)\,(45) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 5 & 4 & 6 & 2 \end{pmatrix},$$

si cette substitution est de degré 7.

Soit une substitution de degré n et soit s la somme du nombre de ses cycles indépendants et de celui de ses éléments conservés [1]. La différence $n - s$ est appelée *décrément* de cette substitution. Il est clair que le décrément est la différence du nombre des éléments non conservés et de celui des cycles indépendants dans la décomposition de la substitution considérée. Pour les exemples 1), 2) et 3) ci-dessus, le décrément est respectivement 3, 4 et 4.

La parité d'une substitution coïncide avec celle de son décrément.

En effet, tout cycle de longueur k se décompose de la manière suivante en un produit de $(k - 1)$ transpositions:

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2)(i_1, i_3) \ldots (i_1, i_k).$$

Supposons maintenant qu'une substitution A soit décomposée en un produit de cycles indépendants. Utilisant la représentation ci-dessus pour chaque cycle intervenant dans l'expression de A, nous obtenons la décomposition de la substitution A en un produit de transpositions. Il est clair que le nombre de ces transpositions est égal à la différence du nombre des éléments non conservés par A et de celui des cycles indépendants dans l'expression correspondante de cette substitution. Il en résulte que A peut être décomposée en un produit de transpositions dont le nombre coïncide avec le décrément; par conséquent, la parité de la substitution A coïncide avec celle de son décrément.

§ 4. Déterminants d'ordre n

Nous voulons à présent généraliser, pour tout n, les résultats obtenus au § 2 pour $n = 2$ et 3. Il nous faut pour cela introduire les déterminants d'ordre n. Or, il est impossible de le faire par le procédé employé dans le cas des déterminants d'ordres 2 et 3, c'est-à-dire par la résolution des systèmes d'équations linéaires, car les calculs deviennent de plus en plus laborieux au fur et à mesure que n augmente et pour n assez grand ils sont pratiquement irréalisables. Nous allons utiliser une autre méthode: partant des déterminants d'ordres 2 et 3, nous tâcherons de trouver la loi générale selon laquelle les déterminants s'expriment au moyen des éléments des matrices correspondantes et nous utiliserons cette loi pour définir les déterminants d'ordre n. Nous démontrerons ensuite que les formules de Cramer, avec les déterminants d'ordre n ainsi définis, restent valables.

Rappelons les expressions des déterminants d'ordres 2 et 3 en fonction des éléments des matrices correspondantes:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21},$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - \\ - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

[1] On pourrait faire correspondre à tout élément conservé par une substitution un cycle de « longueur » 1; par exemple, dans l'exemple 2) ci-dessus on aurait pu écrire: (156) (38) (47) (2). Toutefois, par la suite nous ne le ferons pas.

Nous constatons que tout terme du déterminant d'ordre 2 est le produit de deux éléments appartenant à des colonnes et à des lignes distinctes. En outre, tous les produits, c'est-à-dire tous les termes qu'on puisse former de cette manière à partir des éléments de la matrice d'ordre 2 (ils sont au nombre de deux), interviennent dans la somme qui représente le déterminant. De même, tout terme du déterminant d'ordre 3 est le produit de trois éléments appartenant à des lignes et à des colonnes distinctes. En outre, tous les produits de ce genre interviennent dans l'expression du déterminant.

Soit à présent une matrice carrée d'ordre n

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}. \tag{1}$$

Formons tous les produits possibles de n éléments de la matrice appartenant à des lignes et à des colonnes distinctes. Autrement dit, considérons tous les produits de la forme

$$a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n}, \tag{2}$$

les indices $\alpha_1, \alpha_2, \dots, \alpha_n$ formant une permutation quelconque des nombres $1, 2, \dots, n$. Le nombre de tels produits est égal à celui de toutes les permutations de n éléments, c'est-à-dire à $n!$. Tous ces produits interviennent dans l'expression du déterminant d'ordre n correspondant à la matrice (1).

Pour déterminer le signe avec lequel le produit (2) intervient dans la composition d'un déterminant, notons qu'à l'aide des indices de ce produit on peut former la substitution

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}, \tag{3}$$

c'est-à-dire i devient α_i si le produit (2) contient l'élément situé à l'intersection de la $i^{\text{ème}}$ ligne et de la $\alpha_i^{\text{ème}}$ colonne de la matrice (1). Revenant aux déterminants d'ordres 2 et 3 nous constatons que les produits intervenant dans leurs expressions sont munis du signe $+$ ou $-$ selon que les indices de leurs éléments forment une substitution paire ou impaire. Il est logique de conserver cette loi pour la définition des déterminants d'ordre n.

Ainsi nous sommes conduits à la définition suivante: on appelle *déterminant d'ordre n* associé à la matrice (1) une somme algébrique de $n!$ termes formée d'après la loi suivante: chaque terme de la somme est le produit de n éléments distincts, dont les indices définissent une substitution, ce produit étant muni du signe $+$ si la

substitution est paire et du signe — dans le cas contraire ; en outre, la somme est étendue sur toutes les substitutions distinctes de n éléments.

De même que pour les déterminants d'ordres 2 et 3, nous utilisons le symbole

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \tag{4}$$

pour désigner le déterminant d'ordre n, associé à la matrice (1).

Les déterminants d'ordre n pour $n = 2$ et 3 coïncident avec les déterminants du deuxième et du troisième ordre définis au § 2 ; si $n = 1$, c'est-à-dire si la matrice est composée d'un seul élément, le déterminant est égal à cet élément. Il n'est pas encore évident que nous pourrons appliquer les déterminants d'ordre n, $n > 3$, à la résolution des systèmes d'équations linéaires. On le montrera au § 7 ; préalablement il faut donner une étude détaillée des déterminants et, en particulier, trouver des méthodes qui permettent de les calculer. Cela est d'autant plus nécessaire qu'utiliser directement leur définition pour le calcul des déterminants d'ordre n est assez laborieux, même si n est relativement petit.

Maintenant, nous allons établir quelques propriétés simples des déterminants d'ordre n, se rapportant, de préférence, à l'un des deux problèmes suivants : d'une part, quelles sont les conditions pour qu'un déterminant d'ordre n s'annule et, d'autre part, quelles sont les transformations d'une matrice qui conservent son déterminant sinon le modifient de façon qu'on puisse facilement en tenir compte.

Une matrice est dite *transposée* de la matrice (1) si ses lignes coïncident avec les colonnes correspondantes de la matrice (1) et inversement, autrement dit, la transposée de la matrice (1) est la matrice

$$\begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{pmatrix}. \tag{5}$$

On peut dire, par abus de langage, que la transformation faisant correspondre à la matrice (1) sa transposée est une rotation de la matrice (1) autour de sa diagonale principale. De même, on appelle déterminant transposé le déterminant de la matrice transposée ;

ce déterminant est de la forme:

$$\begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{vmatrix}. \tag{6}$$

Propriété 1. *Un déterminant coïncide avec son transposé.*

En effet, chaque terme du déterminant (4) est de la forme:

$$a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n}, \tag{7}$$

les indices $\alpha_1, \alpha_2, \dots, \alpha_n$ formant une certaine permutation des éléments $1, 2, \dots, n$. Or, tous les facteurs du produit (7) appartiennent à des lignes et à des colonnes distinctes du déterminant (6), et, par conséquent, le produit (7) est un des termes du déterminant transposé. Evidemment, la réciproque est également vraie, de sorte que les déterminants (4) et (6) contiennent les mêmes termes. Le signe du produit (7) dans l'expression du déterminant (4) dépend de la parité de la substitution

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}; \tag{8}$$

dans le déterminant (6) les premiers indices indiquent le numéro de la colonne, les seconds indices celui de la ligne, donc le terme (7) dans le déterminant (6) correspond à la substitution

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix}. \tag{9}$$

Bien que les substitutions (8) et (9) soient, en général, différentes, leur parité est, évidemment, la même, de sorte que le terme (7) est muni du même signe dans l'expression des deux déterminants. Ainsi, les déterminants (4) et (6) sont exprimés par la somme de termes identiques et, par conséquent, coïncident.

Il découle de la propriété 1 que toute proposition concernant les lignes d'un déterminant est également valable pour ses colonnes et inversement. Autrement dit, *les lignes et les colonnes d'un déterminant jouent exactement le même rôle* (contrairement aux lignes et aux colonnes d'une matrice). Tenant compte de ce fait nous n'énonçons et ne montrons les propriétés 2-9 des déterminants que pour les lignes, étant donné que les propriétés analogues pour les colonnes n'exigent point de démonstration.

Propriété 2. *Un déterminant est nul, si tous les éléments d'une de ses lignes sont nuls.*

En effet, supposons que tous les éléments de la $i^{\text{ème}}$ ligne du déterminant soient nuls. Etant donné que chaque terme du déterminant comprend un élément et un seul de la $i^{\text{ème}}$ ligne, tous les termes sont donc nuls.

Propriété 3. *En échangeant deux lignes quelconques d'un déterminant on obtient un déterminant dont les termes sont les mêmes que ceux du déterminant initial mais munis de signe opposé. Autrement dit, en échangeant deux lignes quelconques d'un déterminant, ce dernier change de signe.*

En effet, supposons que l'on ait échangé entre elles la $i^{\text{ème}}$ et la $j^{\text{ème}}$ ligne d'un déterminant (4), $i \neq j$, et que toutes les autres lignes soient restées à leur place. On obtient le déterminant

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \cdot & \cdot & \cdot & \cdot \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \begin{matrix} \\ \\ (i) \\ \\ (j) \\ \\ \\ \end{matrix} \tag{10}$$

(les parenthèses indiquent les numéros des lignes). Le produit

$$a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n} \tag{11}$$

étant un des termes du déterminant (4), tous ses facteurs appartiennent à des lignes et à des colonnes distinctes du déterminant (10). Ainsi, les déterminants (4) et (10) s'expriment par les mêmes termes. Au terme (11), dans le déterminant (4), correspond la substitution

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_j & \dots & \alpha_n \end{pmatrix}, \tag{12}$$

et dans le déterminant (10) la substitution

$$\begin{pmatrix} 1 & 2 & \dots & j & \dots & i & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_i & \dots & \alpha_j & \dots & \alpha_n \end{pmatrix}. \tag{13}$$

En effet, l'élément $a_{i\alpha_i}$, par exemple, se trouve après la transposition de la $i^{\text{ème}}$ et de la $j^{\text{ème}}$ ligne du déterminant (4) à l'intersection de la $j^{\text{ème}}$ ligne et de la $\alpha_i^{\text{ème}}$ colonne du déterminant (10). La substitution (13) s'obtenant de la substitution (12) par une transposition dans sa première ligne, sa parité est opposée. Il en résulte que tous les termes du déterminant (4) interviennent dans le déterminant (10) munis de signe opposé, c'est-à-dire les déterminants (4) et (10) ont la même valeur absolue mais sont de signes opposés.

Propriété 4. *Un déterminant ayant deux lignes identiques est nul.*

En effet, soit d la valeur de ce déterminant et supposons que ses $i^{\text{ème}}$ et $j^{\text{ème}}$ lignes soient identiques ($i \neq j$). Echangeant ces deux lignes, on obtient, d'après la propriété 3, un déterminant dont la valeur est $-d$. Comme, d'autre part, on échange des lignes identiques, le déterminant, en réalité, conserve sa valeur. Donc, $d = -d$, d'où $d = 0$.

Propriété 5. *En multipliant par un nombre k tous les éléments d'une ligne quelconque d'un déterminant d'ordre n on obtient un déterminant dont la valeur est celle du déterminant initial multipliée par k.*

Supposons que tous les éléments de la $i^{\text{ème}}$ ligne soient multipliés par k. Tout terme du déterminant contient un seul élément de la $i^{\text{ème}}$ ligne, de sorte que chaque terme du déterminant nouveau se trouve multiplié par k, d'où découle la propriété 5.

Cette propriété peut être également énoncée de la manière suivante : *si tous les éléments d'une ligne quelconque d'un déterminant d'ordre n sont multipliés par un nombre k, ce nombre peut être mis en facteur devant le déterminant.*

Propriété 6. *Si les éléments de deux lignes quelconques d'un déterminant sont proportionnels, alors le déterminant est nul.*

En effet, supposons que les éléments de la $j^{\text{ème}}$ ligne d'un déterminant, divisés par le nombre k, donnent les éléments correspondants de la $i^{\text{ème}}$ ligne ($i \neq j$). La propriété 5 montre que le déterminant est égal au produit du nombre k par un déterminant ayant deux lignes identiques, d'où il résulte, vu la propriété 4, que le déterminant initial est nul.

Evidemment la propriété 4 (ainsi que la propriété 2, pour $n > 1$) est un cas particulier de la propriété 6 (pour $k = 1$ et $k = 0$).

Propriété 7. *Si tous les éléments de la $i^{\text{ème}}$ ligne d'un déterminant d'ordre n sont de la forme*

$$a_{ij} = b_j + c_j, \qquad j = 1, \ldots, n,$$

alors le déterminant est la somme de deux déterminants, dont les $i^{\text{èmes}}$ lignes sont composées respectivement des éléments b_j et c_j et toutes les autres lignes sont identiques aux lignes correspondantes du déterminant initial.

En effet, tout terme du déterminant donné peut être représenté sous la forme

$$a_{1\alpha_1}a_{2\alpha_2}\ldots a_{i\alpha_i}\ldots a_{n\alpha_n} = a_{1\alpha_1}a_{2\alpha_2}\ldots(b_{\alpha_i}+c_{\alpha_i})\ldots a_{n\alpha_n} =$$
$$= a_{1\alpha_1}a_{2\alpha_2}\ldots b_{\alpha_i}\ldots a_{n\alpha_n} + a_{1\alpha_1}a_{2\alpha_2}\ldots c_{\alpha_i}\ldots a_{n\alpha_n}.$$

Groupant dans la somme représentant le déterminant donné tous les termes de la forme $a_{1\alpha_1}a_{2\alpha_2}\ldots b_{\alpha_i}\ldots a_{n\alpha_n}$ (munis de mêmes signes que les termes correspondants du déterminant donné), nous obtenons, manifestement, un déterminant dont la $i^{\text{ème}}$ ligne est composée des éléments b_j à la place des a_{ij} et toutes les autres lignes sont identiques aux lignes correspondantes du déterminant initial. De même, la somme algébrique des termes de la forme $a_{1\alpha_1}a_{2\alpha_2}\ldots$ $\ldots c_{\alpha_i}\ldots a_{n\alpha_n}$ n'est autre qu'un déterminant dont la $i^{\text{ème}}$ ligne a pour éléments les c_j et toutes les autres lignes coïncident avec les lignes correspondantes du déterminant donné. Ainsi

$$\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ b_1+c_1 & b_2+c_2 & \ldots & b_n+c_n \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ b_1 & b_2 & \ldots & b_n \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ c_1 & c_2 & \ldots & c_n \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

La propriété 7 s'étend sans difficulté au cas où tout élément de la $i^{\text{ème}}$ ligne est la somme de m termes, $m \geqslant 2$.

On dira que la $i^{\text{ème}}$ ligne d'un déterminant est une *combinaison linéaire* de toutes les autres lignes, s'il existe des nombres k_j, $j = 1, 2, \ldots, i-1, i+1, \ldots, n$, tels que $a_{ij} = k_1a_{1j} + k_2a_{2j} + \ldots + k_{i-1}a_{i-1,j} + k_{i+1,j} + \ldots + k_na_{nj}$, quel que soit j, $j = 1, 2, \ldots, n$. Certains des nombres k_j peuvent être nuls, c'est-à-dire la $i^{\text{ème}}$ ligne est, dans ce cas, une combinaison linéaire seulement de certaines lignes du déterminant et non pas de toutes. Si, en particulier, tous les nombres k_j, excepté un seul, sont nuls, alors on retrouve le cas où les deux lignes d'un déterminant sont proportionnelles. Enfin, si l'une des lignes du déterminant est composée de zéros, alors elle est toujours une combinaison linéaire des autres lignes, car, dans ce cas, tous les k_j sont nuls.

Propriété 8. *Si l'une des lignes d'un déterminant d'ordre n est une combinaison linéaire des autres lignes, alors ce déterminant est nul.*

Supposons, par exemple, que la $i^{\text{ème}}$ ligne soit une combinaison linéaire de s lignes quelconques du déterminant, $1 \leqslant s \leqslant n-1$. Tout élément de la $i^{\text{ème}}$ ligne est dans ce cas une somme de s termes. Utilisant la propriété 7, décomposons notre déterminant en une somme de déterminants dont chacun possède une ligne identique à sa $i^{\text{ème}}$ ligne. D'après la propriété 6, tous ces déterminants sont nuls, de sorte que le déterminant initial l'est aussi.

Cette propriété est une extension de la propriété 6. En outre, il sera prouvé au § 10 qu'elle représente le cas général où un déterminant d'ordre n est nul.

Propriété 9. *Un déterminant d'ordre n ne varie pas si l'on ajoute aux éléments de l'une de ses lignes les éléments correspondants d'une autre ligne, multipliés par un même nombre.*

En effet, supposons que la valeur d'un déterminant soit d et que l'on ajoute aux éléments de la $i^{\text{ème}}$ ligne les éléments correspondants de la $j^{\text{ème}}$ ligne multipliés par un nombre k. Autrement dit, tout élément de la $i^{\text{ème}}$ ligne du déterminant obtenu de cette manière est de la forme $a_{is} + ka_{js}$, $s = 1, 2, \ldots, n$, $i \neq j$. Selon la propriété 7, le déterminant est égal à la somme de deux déterminants dont le premier est égal à d et le second, possédant deux lignes proportionnelles, est donc nul.

Le nombre k pouvant être négatif, il en résulte qu'*en retranchant d'une ligne quelconque une autre ligne multipliée par un nombre quelconque d'un déterminant d'ordre n, la valeur de ce dernier ne change pas.* Plus généralement, un *déterminant d'ordre n ne change pas si l'on ajoute à l'une de ses lignes une combinaison linéaire quelconque des autres lignes.*

Considérons un exemple. Un déterminant est dit *antisymétrique* si les éléments symétriques par rapport à la diagonale principale ont les mêmes valeurs absolues mais sont de signes opposés. Autrement dit, les éléments d'un déterminant antisymétrique doivent vérifier, pour tous i et j, les égalités $a_{ji} = -a_{ij}$. Il en résulte, en particulier, que $a_{ii} = -a_{ii} = 0$ pour tous i. Ainsi. tout déterminant antisymétrique est de la forme:

$$d = \begin{vmatrix} 0 & a_{12} & a_{13} & \ldots & a_{1n} \\ -a_{12} & 0 & a_{23} & \ldots & a_{2n} \\ -a_{13} & -a_{23} & 0 & \ldots & a_{3n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_{1n} & -a_{2n} & -a_{3n} & \ldots & 0 \end{vmatrix}$$

Multipliant chaque ligne de ce déterminant par le nombre -1, nous obtenons un déterminant qui est le transposé du précédent, c'est-à-dire le même que le déterminant initial. Il en résulte, en vertu de la propriété 5, que

$$(-1)^n d = d.$$

Si n est impair il en découle que $-d = d = 0$. Donc, *tout déterminant antisymétrique d'ordre impair est nul.*

§ 5. Mineurs et cofacteurs

Comme il a été mentionné au paragraphe précédent, il serait difficile de calculer les déterminants d'ordre n en s'appuyant sur leur définition, c'est-à-dire en écrivant chaque fois tous les $n!$ termes munis de signes correspondants. Il existe d'autres méthodes de calcul, plus simples. Elles sont basées sur le fait qu'un déterminant d'ordre n peut être exprimé par des déterminants d'ordres inférieurs à n. Pour trouver les formules correspondantes introduisons une notion.

Soient d un déterminant d'ordre n et k un nombre entier tel que $1 \leqslant k \leqslant n-1$. Fixons k lignes et k colonnes quelconques du déterminant d. Les éléments situés à leurs intersections, c'est-à-dire les éléments qui appartiennent à l'une des k lignes et à l'une des k colonnes choisies, forment manifestement une matrice carrée d'ordre k. Le déterminant de cette matrice est appelé *mineur d'ordre* k du déterminant d. Autrement dit, tout déterminant qui s'obtient en y supprimant $n-k$ lignes et $n-k$ colonnes quelconques est appelé mineur d'ordre k du déterminant d. Notamment, en supprimant une ligne et une colonne quelconques d'un déterminant nous obtenons un mineur d'ordre $n-1$; d'autre part, tout élément du déterminant d est un mineur du premier ordre.

Soit M un mineur d'ordre k d'un déterminant d d'ordre n. En supprimant les lignes et les colonnes qui engendrent M, on obtient, évidemment, un mineur M' d'ordre $n-k$ qui est appelé *mineur complémentaire* de M. Inversement, en supprimant les lignes et les colonnes qui forment M', on retrouve le mineur M. Ainsi, on peut parler d'un *couple de mineurs* du déterminant d qui sont *complémentaires l'un par rapport à l'autre*. En particulier, l'élément a_{ij} et le mineur d'ordre $n-1$ qui s'obtient du déterminant d en supprimant la $i^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne sont complémentaires l'un par rapport à l'autre.

Soient $i_1, i_2, \ldots, i_k$ et $j_1, j_2, \ldots, j_k$ les indices respectivement des lignes et des colonnes formant le mineur M d'ordre k. Le mineur complémentaire M' muni du signe plus ou moins, selon la parité de la somme:

$$s_M = i_1 + i_2 + \ldots + i_k + j_1 + j_2 + \ldots + j_k, \tag{1}$$

est appelé *cofacteur* du mineur M. Autrement dit, le cofacteur d'un mineur M est le nombre $(-1)^{s_M} M'$.

Le produit d'un mineur quelconque M par son cofacteur dans un déterminant d est une somme algébrique dont les termes qui s'obtiennent en multipliant les termes du mineur M par les termes du mineur complémentaire M' munis du signe $(-1)^{s_M}$ sont certains termes du déterminant

d; en outre, leurs signes dans cette somme coïncident avec les signes dont ils sont munis dans la composition du déterminant.

Commençons la démonstration de ce théorème par le cas où le mineur M est formé des k premières lignes et des k premières colonnes du déterminant d:

$$d=\left|\begin{array}{ccc|ccc} a_{11} & \ldots & a_{1k} & a_{1,k+1} & \ldots & a_{1n} \\ \ldots & M & \ldots & \ldots & \ldots & \ldots \\ a_{k1} & \ldots & a_{kk} & a_{k,k+1} & \ldots & a_{kn} \\ \hline a_{k+1,1} & \ldots & a_{k+1,k} & a_{k+1,k+1} & \ldots & a_{k+1,n} \\ \ldots & \ldots & \ldots & \ldots & M' & \ldots \\ a_{n1} & \ldots & a_{nk} & a_{n,k+1} & \ldots & a_{nn} \end{array}\right|.$$

Ici le mineur M' est engendré par les $(n-k)$ lignes et les $(n-k)$ colonnes d'indices $k+1, \ldots, n$. Le nombre s_M

$$s_M = 1+2+\ldots+k+1+2+\ldots+k = 2(1+2+\ldots+k)$$

est pair dans ce cas, c'est-à-dire le cofacteur de M est le mineur M'. Soit

$$a_{1\alpha_1}a_{2\alpha_2}\ldots a_{k\alpha_k} \tag{2}$$

un terme quelconque du mineur M; son signe dans l'expression de M est $(-1)^l$, où l est le nombre d'inversions dans la substitution

$$\begin{pmatrix} 1 & 2 & \ldots & k \\ \alpha_1 & \alpha_2 & \ldots & \alpha_k \end{pmatrix}. \tag{3}$$

Soit

$$a_{k+1,\beta_{k+1}}a_{k+2,\beta_{k+2}}\ldots a_{n\beta_n} \tag{4}$$

un terme quelconque du mineur M'. Son signe est $(-1)^{l'}$, où l' est le nombre d'inversions dans la substitution

$$\begin{pmatrix} k+1 & k+2 & \ldots & n \\ \beta_{k+1} & \beta_{k+2} & \ldots & \beta_n \end{pmatrix}. \tag{5}$$

Multipliant (2) par (4), on obtient le produit de n éléments

$$a_{1\alpha_1}a_{2\alpha_2}\ldots a_{k\alpha_k}a_{k+1,\beta_{k+1}}a_{k+2,\beta_{k+2}}\ldots a_{n\beta_n} \tag{6}$$

qui appartiennent à des lignes et à des colonnes distinctes du déterminant d; le produit (6) est donc un des termes du déterminant d. Il est clair que le signe dont est muni le terme (6) dans le produit $M \cdot M'$ est le produit des signes des termes (2) et (4), c'est-à-dire $(-1)^l \cdot (-1)^{l'} = (-1)^{l+l'}$. Le terme (6) est muni du même signe

dans le déterminant d. En effet, la seconde ligne de la substitution

$$\begin{pmatrix} 1 & 2 & \dots & k & k+1 & k+2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_k & \beta_{k+1} & \beta_{k+2} & \dots & \beta_n \end{pmatrix},$$

formée par les indices des facteurs du terme (6), n'a que $l + l'$ inversions, car aucun des indices α ne peut former une inversion avec aucun des indices β: rappelons que tous les $\alpha \leqslant k$ et $\beta \geqslant k + 1$.

Ainsi, le cas particulier du théorème énoncé ci-dessus est prouvé. Passons maintenant au cas général. Supposons que le mineur M soit situé à l'intersection des lignes d'indices $i_1, \dots, i_k$ et des colonnes d'indices $j_1, \dots, j_k$. Supposons, en outre, que

$$i_1 < i_2 < \dots < i_k, \qquad j_1 < j_2 < \dots < j_k.$$

Echangeant des lignes et des colonnes, tâchons de faire passer le mineur M dans l'angle gauche supérieur du déterminant et cela de façon que le mineur complémentaire soit conservé. Pour cela échangeons la $i_1^{\text{ème}}$ et la $(i_1 - 1)^{\text{ème}}$ ligne, ensuite la $i_1^{\text{ème}}$ et la $(i_1 - 2)^{\text{ème}}$, etc., jusqu'à ce que la $i_1^{\text{ème}}$ ligne prenne la place de la première; pour aboutir à ce résultat il faut, évidemment, transposer $(i_1 - 1)$ fois les lignes. Echangeons maintenant de la même façon la $i_2^{\text{ème}}$ ligne et toutes les autres qui la précèdent jusqu'à ce qu'elle prenne la place de la seconde ligne du déterminant. Comme il est facile de le voir, il faut pour cela transposer $(i_2 - 2)$ fois les lignes. Faisons passer, d'une manière analogue, la $i_3^{\text{ème}}$ ligne à la place de la troisième et ainsi de suite, jusqu'à ce que la $i_k^{\text{ème}}$ ligne prenne la place de la $k^{\text{ème}}$. Le nombre total de transpositions de lignes, que nous avons eu à accomplir pour aboutir à ce résultat, est

$$(i_1 - 1) + (i_2 - 2) + \dots + (i_k - k) =$$
$$= (i_1 + i_2 + \dots + i_k) - (1 + 2 + \dots + k).$$

Après ces transpositions le mineur M se trouve à l'intersection des k premières lignes et des colonnes d'indices $j_1, \dots, j_k$. Echangeons maintenant successivement la $j_1^{\text{ème}}$ colonne et toutes celles qui la précèdent jusqu'à ce que la $j_1^{\text{ème}}$ colonne occupe la place de la première; ensuite la $j_2^{\text{ème}}$ et les colonnes précédentes jusqu'à ce que la $j_2^{\text{ème}}$ colonne prenne la place de la deuxième et ainsi de suite. Pour aboutir à ce résultat il faut transposer les colonnes

$$(j_1 + j_2 + \dots + j_k) - (1 + 2 + \dots + k)$$

fois.

L'application de ces transformations nous conduit à un déterminant d' dans lequel le mineur M se trouve à la même place que dans le cas particulier considéré au début de la démonstration. Comme

nous n'avons échangé chaque fois que des lignes et des colonnes voisines, les lignes et les colonnes formant le mineur M' ont conservé leurs places respectives. Par conséquent, le mineur M, en tant que mineur du déterminant d', a pour complémentaire le mineur M' qui, cette fois, est situé dans l'angle droit inférieur du déterminant d'. Comme nous l'avons déjà démontré, le produit $M \cdot M'$ est égal à la somme d'un certain nombre de termes du déterminant d' munis des mêmes signes qu'ont ces termes dans le déterminant d'. Or, le nombre total de transpositions des lignes et des colonnes qui nous ont conduits du déterminant d au déterminant d' est égal à

$$\begin{aligned}&[(i_1+i_2+\ldots+i_k)-(1+2+\ldots+k)]+\\&+[(j_1+j_2+\ldots+j_k)-(1+2+\ldots+k)]=\\&=s_M-2(1+2+\ldots+k).\end{aligned}$$

Par conséquent, en vertu des résultats du paragraphe précédent, chaque terme du déterminant d' est égal à son homologue dans le déterminant d, multiplié par $(-1)^{s_M}$ (évidemment, le nombre pair $2(1+2+\ldots+k)$ n'influe pas sur le signe). Il en résulte que le produit $(-1)^{s_M} M \cdot M'$ est une somme d'un certain nombre de termes intervenant dans l'expression du déterminant d, ces termes étant munis exactement des mêmes signes que dans l'expression du déterminant d. Le théorème est prouvé.

Faisons une remarque. Soient deux mineurs M et M', complémentaires l'un par rapport à l'autre; alors les nombres s_M et $s_{M'}$ ont la même parité. En effet, l'indice de toute ligne (ou colonne) n'intervient que dans l'une des sommes représentant les nombres s_M et $s_{M'}$. Par conséquent, $s_M+s_{M'}$ est la somme des indices de toutes les lignes et colonnes du déterminant, c'est-à-dire le nombre pair $2(1+2+\ldots+n)$.

§ 6. Calcul des déterminants

Les résultats du paragraphe précédent permettent de ramener le problème du calcul d'un déterminant d'ordre n à celui du calcul d'un certain nombre de déterminants d'ordre $(n-1)$. Introduisons d'abord les notations suivantes: on désigne par M_{ij} le mineur complémentaire de l'élément a_{ij} du déterminant d d'ordre n (on l'appellera tout simplement *mineur de l'élément* a_{ij}), autrement dit M_{ij} est le mineur d'ordre $(n-1)$, qui s'obtient en supprimant la $i^{\text{ème}}$ ligne et la $j^{\text{ème}}$ colonne du déterminant d. Le cofacteur de a_{ij} sera noté A_{ij}, c'est-à-dire

$$A_{ij}=(-1)^{i+j}M_{ij}.$$

Comme il a été montré au paragraphe précédent, le produit $a_{ij}A_{ij}$ est égal à la somme de plusieurs termes intervenant dans le déterminant d; en outre, ces termes ont les mêmes signes que dans le déterminant. Il est facile de calculer le nombre des termes figurant dans le produit $a_{ij}A_{ij}$: il est égal au nombre des termes contenus dans le mineur M_{ij}, c'est-à-dire à $(n-1)!$.

Soit une ligne quelconque d'un déterminant d, par exemple, la $i^{\text{ème}}$; formons les produits des éléments de la $i^{\text{ème}}$ ligne par leurs cofacteurs respectifs:

$$a_{i1}A_{i1},\ a_{i2}A_{i2},\ \ldots,\ a_{in}A_{in}. \tag{1}$$

Chaque terme du déterminant d n'intervient que dans un et seulement un des produits (1). En effet, chaque terme du déterminant d intervenant dans le produit $a_{i1}A_{i1}$ a pour facteur l'élément a_{i1} de la $i^{\text{ème}}$ ligne et, par conséquent, est distinct de tout terme des produits $a_{i2}A_{i2}$, ces derniers contenant tous un autre élément de la $i^{\text{ème}}$ ligne, à savoir a_{i2}, etc.

D'autre part, le nombre total des termes du déterminant d, intervenant dans tous les produits (1), est

$$(n-1)!\cdot n = n!,$$

autrement dit, on retrouve tous les termes du déterminant d. Ainsi, nous avons démontré qu'un *déterminant d* peut être *développé* de la manière suivante *par rapport à la $i^{\text{ème}}$ ligne*:

$$d = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in}, \tag{2}$$

c'est-à-dire *le déterminant d est égal à la somme des produits des éléments d'une ligne quelconque par les cofacteurs correspondants.* Evidemment, on a un développement analogue par rapport aux éléments d'une colonne quelconque du déterminant d.

Remplaçant dans la formule (2) les cofacteurs par les mineurs correspondants munis des signes plus ou moins, *le problème du calcul d'un déterminant d'ordre n se ramène à celui du calcul d'un certain nombre de déterminants d'ordre* $(n-1)$. Evidemment, si la $i^{\text{ème}}$ ligne possède des éléments nuls, il n'y a aucun besoin de calculer les mineurs correspondants. Ceci dit, il est donc commode de transformer d'abord le déterminant, en utilisant la propriété 9 (cf. § 4), de manière que l'une des lignes ou l'une des colonnes ait de nombreux éléments nuls. En réalité, *la propriété 9 permet de transformer un déterminant d'ordre n de manière que tous les éléments d'une ligne ou d'une colonne quelconque, sauf un, soient nuls.* En effet, si $a_{ik} \neq 0$, alors tout élément a_{ij}, $j \neq k$, peut être remplacé par l'élément nul à la suite de la transformation suivante: on retranche de la $j^{\text{ème}}$ colonne la $k^{\text{ème}}$ colonne multipliée par $\frac{a_{ij}}{a_{ik}}$. Ainsi, on peut ramener

le calcul d'un déterminant d'ordre n à celui d'un *seul* déterminant d'ordre $(n-1)$.

Exemples.

1. Calculer le déterminant du quatrième ordre

$$d=\begin{vmatrix} 3 & 1 & -1 & 2 \\ -5 & 1 & 3 & -4 \\ 2 & 0 & 1 & -1 \\ 1 & -5 & 3 & -3 \end{vmatrix}.$$

La troisième ligne de ce déterminant ayant un élément nul, il y a intérêt à le développer par rapport aux éléments de cette ligne. Il vient :

$$d=(-1)^{3+1}\cdot 2\cdot\begin{vmatrix} 1 & -1 & 2 \\ 1 & 3 & -4 \\ -5 & 3 & -3 \end{vmatrix}+$$

$$+(-1)^{3+3}\cdot 1\cdot\begin{vmatrix} 3 & 1 & 2 \\ -5 & 1 & -4 \\ 1 & -5 & -3 \end{vmatrix}+(-1)^{3+4}\cdot(-1)\cdot\begin{vmatrix} 3 & 1 & -1 \\ -5 & 1 & 3 \\ 1 & -5 & 3 \end{vmatrix}.$$

Calculant les déterminants du troisième ordre, on obtient :

$$d=2\cdot 16-40+48=40.$$

2. Calculer le déterminant d'ordre 5 :

$$d=\begin{vmatrix} -2 & 5 & 0 & -1 & 3 \\ 1 & 0 & 3 & 7 & -2 \\ 3 & -1 & 0 & 5 & -5 \\ 2 & 6 & -4 & 1 & 2 \\ 0 & -3 & -1 & 2 & 3 \end{vmatrix}.$$

Ajoutant à la seconde ligne la cinquième ligne multipliée par 3 et retranchant ensuite de la quatrième ligne la cinquième ligne multipliée par 4, il vient :

$$d=\begin{vmatrix} -2 & 5 & 0 & -1 & 3 \\ 1 & -9 & 0 & 13 & 7 \\ 3 & -1 & 0 & 5 & -5 \\ 2 & 18 & 0 & -7 & -10 \\ 0 & -3 & -1 & 2 & 3 \end{vmatrix}.$$

Développant ce déterminant par rapport aux éléments de la troisième colonne qui n'a qu'un élément non nul (la somme des indices de cet élément est $5+3$,

c'est-à-dire un nombre pair), il vient:

$$d=(-1)\cdot\begin{vmatrix} -2 & 5 & -1 & 3 \\ 1 & -9 & 13 & 7 \\ 3 & -1 & 5 & -5 \\ 2 & 18 & -7 & -10 \end{vmatrix}.$$

Transformons le déterminant obtenu, en ajoutant à sa première ligne la seconde ligne multipliée par 2 et retranchant de sa troisième ligne la seconde ligne multipliée par 3 et de sa quatrième ligne la seconde ligne multipliée par 2; il vient:

$$d=-\begin{vmatrix} 0 & -13 & 25 & 17 \\ 1 & -9 & 13 & 7 \\ 0 & 26 & -34 & -26 \\ 0 & 36 & -33 & -24 \end{vmatrix};$$

développant ce dernier déterminant par rapport aux éléments de sa première colonne et remarquant que l'unique élément non nul de cette colonne a pour somme des indices un nombre impair, nous obtenons:

$$d=\begin{vmatrix} -13 & 25 & 17 \\ 26 & -34 & -26 \\ 36 & -33 & -24 \end{vmatrix}.$$

Calculons ce déterminant d'ordre 3 en le développant par rapport aux éléments de sa troisième ligne; il vient:

$$d=36\cdot\begin{vmatrix} 25 & 17 \\ -34 & -26 \end{vmatrix}-(-33)\cdot\begin{vmatrix} -13 & 17 \\ 26 & -26 \end{vmatrix}+(-24)\cdot\begin{vmatrix} -13 & 25 \\ 26 & -34 \end{vmatrix}=$$
$$=36\cdot(-72)-(-33)\cdot(-104)+(-24)\cdot(-208)=-1032.$$

3. *Soit un déterminant d'ordre n. Supposons que tous ses éléments, se trouvant d'un même côté de la diagonale principale, soient nuls. Alors, le déterminant considéré est égal au produit des éléments de sa diagonale principale.*

Pour les déterminants d'ordre deux cette proposition est évidente. Ainsi, par récurrence sur n nous démontrons le cas général; autrement dit, supposons que la proposition soit vraie pour tout déterminant d'ordre $(n-1)$ et démontrons qu'elle est encore vraie pour un déterminant d'ordre n; pour cela considérons

$$d=\begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & a_{33} & \dots & a_{3n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & a_{nn} \end{vmatrix}.$$

Développant ce dernier par rapport aux éléments de la première colonne, l'unique élément non nul de cette colonne étant a_{11} (dont la somme des indices

4*

est paire), nous obtenons :

$$d = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ 0 & a_{33} & \dots & a_{3n} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & a_{nn} \end{vmatrix}.$$

Or, on peut appliquer l'hypothèse de récurrence au mineur dans le second membre de la dernière égalité, son ordre étant $(n-1)$; selon cette hypothèse le mineur en question est égal au produit $a_{22}a_{33} \dots a_{nn}$, de sorte que

$$d = a_{11}a_{22} \dots a_{nn}.$$

4. On appelle *déterminant de Vandermonde* le déterminant

$$d = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{vmatrix}.$$

Montrons que, *quel que soit n, le déterminant de Vandermonde est le produit de toutes les différences* $a_i - a_j$, *avec* $1 \leqslant j < i \leqslant n$. En effet, pour $n = 2$ on a

$$\begin{vmatrix} 1 & 1 \\ a_1 & a_2 \end{vmatrix} = a_2 - a_1.$$

Nous allons raisonner par récurrence sur n. Supposons que notre proposition soit déjà démontrée pour les déterminants de Vandermonde d'ordre $(n-1)$. Transformons le déterminant d de la façon suivante: retranchons de la $n^{\text{ème}}$ ligne de d la $(n-1)^{\text{ème}}$ ligne multipliée par a_1, puis de la $(n-1)^{\text{ème}}$ la $(n-2)^{\text{ème}}$ ligne multipliée par a_1, etc. ; enfin, retranchons de la deuxième ligne de d sa première ligne multipliée par a_1. Nous obtenons:

$$d = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & a_2 - a_1 & a_3 - a_1 & \dots & a_n - a_1 \\ 0 & a_2^2 - a_1a_2 & a_3^2 - a_1a_3 & \dots & a_n^2 - a_1a_n \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & a_2^{n-1} - a_1a_2^{n-2} & a_3^{n-1} - a_1a_3^{n-2} & \dots & a_n^{n-1} - a_1a_n^{n-2} \end{vmatrix}.$$

Développant ce déterminant par rapport aux éléments de sa première colonne, nous sommes conduits à un déterminant d'ordre $(n-1)$; mettant en facteur toutes les différences $a_j - a_1$, $2 \leqslant j \leqslant n$ ($a_j - a_1$ est le facteur commun des éléments de la $(j-1)^{\text{ème}}$ colonne du déterminant d'ordre $(n-1)$ obtenu), le déterminant d prend la forme

$$d = (a_2 - a_1)(a_3 - a_1) \dots (a_n - a_1) \cdot \begin{vmatrix} 1 & 1 & \dots & 1 \\ a_2 & a_3 & \dots & a_n \\ a_2^2 & a_3^2 & \dots & a_n^2 \\ \cdot & \cdot & \cdot & \cdot \\ a_2^{n-2} & a_3^{n-2} & \dots & a_n^{n-2} \end{vmatrix}.$$

Le dernier facteur dans le second membre est le déterminant de Vandermonde d'ordre $(n-1)$, qui, selon l'hypothèse de récurrence, est le produit de toutes les différences $a_i - a_j$ avec $2 \leqslant j < i \leqslant n$. Utilisant le symbole Π pour désigner les produits, on peut écrire la formule

$$d=(a_2-a_1)(a_3-a_1)\ldots(a_n-a_1)\cdot\prod_{2\leq j<i\leq n}(a_i-a_j)=\prod_{1\leq j<i\leq n}(a_i-a_j).$$

On démontre d'une façon analogue que le déterminant

$$d'=\begin{vmatrix} a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \ldots & a_n^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_1^2 & a_2^2 & a_3^2 & \ldots & a_n^2 \\ a_1 & a_2 & a_3 & \ldots & a_n \\ 1 & 1 & 1 & \ldots & 1 \end{vmatrix}$$

est le produit de toutes les différences $a_i - a_j$ avec $1 \leqslant i < j \leqslant n$, c'est-à-dire que

$$d'=\prod_{1\leq i<j\leq n}(a_i-a_j).$$

Le théorème suivant généralise le développement d'un déterminant d'ordre n par rapport aux éléments d'une de ses lignes ou colonnes, obtenu précédemment. Cette généralisation donne un *développement par rapport aux mineurs extraits de plusieurs lignes ou colonnes quelconques d'un déterminant donné d'ordre n.*

Théorème de Laplace. *Soient k lignes (ou k colonnes) quelconques d'un déterminant d d'ordre n avec* $1 \leqslant k \leqslant n-1$. *Alors d est égal à la somme des produits de tous les mineurs d'ordre k extraits des lignes choisies par les cofacteurs correspondants.*

Démonstration. Soient $i_1, i_2, \ldots, i_k$ les indices des lignes fixées du déterminant d. On sait que le produit d'un mineur M d'ordre k de d, extrait de ces lignes, par son cofacteur est une somme de plusieurs termes intervenant dans le déterminant d qui sont pris avec les mêmes signes qu'ils ont dans la composition du déterminant. Le théorème sera donc prouvé si nous montrons que nous obtenons, une fois et seulement une fois, tous les termes du déterminant lorsque M parcourt tous les mineurs d'ordre k extraits des lignes choisies.

Soit

$$a_{1\alpha_1}a_{2\alpha_2}\ldots a_{n\alpha_n} \tag{3}$$

un terme quelconque du déterminant d. Groupons les facteurs du produit (3) appartenant aux lignes $i_1, \ldots, i_k$. Il vient

$$a_{i_1\alpha_{i_1}}a_{i_2\alpha_{i_2}}\ldots a_{i_k\alpha_{i_k}}; \tag{4}$$

k facteurs du produit (4) appartiennent à des colonnes distinctes, à savoir aux colonnes d'indices $\alpha_{i_1}, \ldots, \alpha_{i_k}$. Donc, ces indices sont bien définis dès que l'on se donne un produit de la forme (3). Si on note par M le mineur d'ordre k se trouvant à l'intersection

des colonnes d'indices $\alpha_{i_1}, \ldots, \alpha_{i_k}$ et des lignes d'indices $i_1, \ldots$ $\ldots, i_k$, fixées d'avance, le produit (4) est un des termes du mineur M, tandis que le produit de tous les autres éléments du terme (3) représente un des termes du mineur complémentaire de M dans d. Ainsi, chaque terme du déterminant entre dans le produit d'un mineur d'ordre k, bien déterminé, extrait des lignes choisies, par son mineur complémentaire. Enfin, pour que chaque terme du produit soit muni du même signe que dans le déterminant, il faut, comme on le sait, remplacer le mineur complémentaire par le cofacteur correspondant. Ainsi s'achève la démonstration du théorème.

On aurait pu démontrer le théorème par une autre voie. En effet, le produit d'un mineur M d'ordre k extrait des k lignes choisies par son cofacteur est une somme de $k!\,(n-k)!$ termes, car M en contient $k!$ et son cofacteur, qui, au signe près, coïncide avec le mineur complémentaire d'ordre $(n-k)$ possède $(n-k)!$ termes. D'autre part, le nombre de mineurs distincts d'ordre k qu'on peut extraire de k lignes d'un déterminant d'ordre n est égal au nombre de combinaisons de n éléments k à k, c'est-à-dire à

$$\frac{n!}{k!\,(n-k)!}.$$

Il en résulte que la somme de tous les produits des mineurs d'ordre k extraits des k lignes fixées par leurs cofacteurs respectifs comprend exactement $n!$ termes. Or, le déterminant d en contient autant. Le théorème sera donc prouvé si nous montrons que chaque terme du déterminant d intervient au moins une fois dans la somme des produits en question. Nous laissons au lecteur le soin de répéter avec certaines simplifications les raisonnements donnés dans la démonstration précédente.

Le théorème de Laplace permet de ramener le problème du calcul d'un déterminant d'ordre n à celui du calcul d'un certain nombre de déterminants d'ordre k et $n-k$. En général ce nombre est assez grand, c'est pourquoi l'application du théorème de Laplace n'est utile que dans les cas où l'on peut choisir les k lignes (ou colonnes) du déterminant donné de manière que de nombreux mineurs d'ordre k extraits de ces lignes soient nuls.

Exemples.

1. Soit un déterminant dont les éléments qui se trouvent à l'intersection des k premières lignes et des $(n-k)$ dernières colonnes sont tous nuls:

$$d=\begin{vmatrix} a_{11} & \ldots & a_{1k} & & & \\ \ldots & \ldots & \ldots & & 0 & \\ a_{k1} & \ldots & a_{kk} & & & \\ a_{k+1,1} & \ldots & a_{k+1,k} & a_{k+1,k+1} & \ldots & a_{k+1,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nk} & a_{n,k+1} & \ldots & a_{nn} \end{vmatrix}.$$

Alors le déterminant est égal au produit de deux mineurs:

$$d=\begin{vmatrix} a_{11} & \dots & a_{1k} \\ \cdot & \cdot\;\cdot & \cdot \\ a_{k1} & \dots & a_{kk} \end{vmatrix} \cdot \begin{vmatrix} a_{k+1,\,k+1} & \dots & a_{k+1,\,n} \\ \cdot & \cdot\;\cdot\;\cdot & \cdot \\ a_{n,\,k+1} & \dots & a_{nn} \end{vmatrix}.$$

Pour démontrer cette formule il suffit de développer le déterminant d par rapport aux mineurs des k premières lignes.

2. Soit d un déterminant d'ordre $2n$ dont le mineur d'ordre n formé par les n premières lignes et les n premières colonnes a tous les éléments nuls. Notant respectivement par M, M' et M'' les mineurs d'ordre n formés par les n premières lignes et les n dernières colonnes, ensuite par les n dernières lignes et les n premières colonnes et, enfin, par les n dernières lignes et les n dernières colonnes, le déterminant d s'écrit symboliquement comme suit: $d=\begin{vmatrix} 0 & M \\ M' & M'' \end{vmatrix}$, d'où $d=$ $=(-1)^n MM'$.

Pour le montrer, il suffit de développer le déterminant d par rapport aux mineurs d'ordre n extraits des n premières lignes. Le résultat est immédiat, étant donné que

$$s_M=(1+2+\dots+n)+[(n+1)+(n+2)\dots+2n]=n+2n^2,$$

de sorte que s_M et n ont la même parité.

3. Calculer le déterminant

$$d=\begin{vmatrix} -4 & 1 & 2 & -2 & 1 \\ 0 & 3 & 0 & 1 & -5 \\ 2 & -3 & 1 & -3 & 1 \\ -1 & -1 & 3 & -1 & 0 \\ 0 & 4 & 0 & 2 & 5 \end{vmatrix}.$$

Développant ce dernier par rapport aux mineurs de la première et de la troisième colonne (ces colonnes ayant les éléments nuls convenablement placés) il vient:

$$d=(-1)^{1+3+1+3}\begin{vmatrix} -4 & 2 \\ 2 & 1 \end{vmatrix} \cdot \begin{vmatrix} 3 & 1 & -5 \\ -1 & -1 & 0 \\ 4 & 2 & 5 \end{vmatrix} +$$

$$+(-1)^{1+4+1+3}\begin{vmatrix} -4 & 2 \\ -1 & 3 \end{vmatrix} \cdot \begin{vmatrix} 3 & 1 & -5 \\ -3 & -3 & 1 \\ 4 & 2 & 5 \end{vmatrix} +$$

$$+(-1)^{3+4+1+3}\begin{vmatrix} 2 & 1 \\ -1 & 3 \end{vmatrix} \cdot \begin{vmatrix} 1 & -2 & 1 \\ 3 & 1 & -5 \\ 4 & 2 & 5 \end{vmatrix} =$$

$$=(-8)\cdot(-20)-(-10)\cdot(-62)-7\cdot 87=-1069.$$

§ 7. Règle de Cramer

Les déterminants d'ordre n, introduits dans le paragraphe précédent de façon analogue aux déterminants d'ordres 2 et 3, peuvent être utilisés, tout comme ces derniers, pour la résolution des systèmes

d'équations linéaires. Faisons d'abord une remarque supplémentaire concernant le développement d'un déterminant par rapport aux éléments de l'une de ses lignes ou de l'une de ses colonnes; ultérieurement cette remarque sera utilisée plus d'une fois.

Développons le déterminant

$$d = \begin{vmatrix} a_{11} & \ldots & a_{1j} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2j} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \ldots & a_{nj} & \ldots & a_{nn} \end{vmatrix}$$

par rapport aux éléments de sa $j^{\text{ème}}$ colonne:

$$d = a_{1j}A_{1j} + a_{2j}A_{2j} + \ldots + a_{nj}A_{nj},$$

et remplaçons dans ce développement les éléments de la $j^{\text{ème}}$ colonne par n nombres arbitraires $b_1, b_2, \ldots, b_n$. Bien entendu, l'expression

$$b_1A_{1j} + b_2A_{2j} + \ldots + b_nA_{nj},$$

que nous obtenons après cette transformation, représente le développement du déterminant d':

$$d' = \begin{vmatrix} a_{11} & \ldots & b_1 & \ldots & a_{1n} \\ a_{21} & \ldots & b_2 & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix},$$

par rapport aux éléments de sa $j^{\text{ème}}$ colonne; d' s'obtient de d en y remplaçant les éléments de la $j^{\text{ème}}$ colonne par $b_1, b_2, \ldots, b_n$. En effet, cette transformation conserve les mineurs complémentaires des éléments de la $j^{\text{ème}}$ colonne et, par conséquent, les cofacteurs de ces éléments.

On va utiliser cette remarque dans le cas où les nombres b_1, $b_2, \ldots, b_n$ ont pour valeurs respectives les éléments de la $k^{\text{ème}}$ colonne du déterminant d, $k \neq j$. Le déterminant d' correspondant est, dans ce cas, nul, car il a deux colonnes identiques, de sorte qu'il en est de même pour son développement par rapport aux éléments de sa $j^{\text{ème}}$ colonne:

$$a_{1k}A_{1j} + a_{2k}A_{2j} + \ldots + a_{nk}A_{nj} = 0 \text{ pour } j \neq k.$$

Ainsi, *la somme des produits de tous les éléments d'une colonne quelconque par les cofacteurs des éléments correspondants est nulle.* Evidemment, le même résultat est vrai pour les *lignes.*

Passons maintenant à l'étude des systèmes d'équations linéaires, en nous bornant dans ce paragraphe aux systèmes ayant *le même nombre d'équations que d'inconnues*, c'est-à-dire aux systèmes de la

forme

$$\left.\begin{aligned} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n&=b_1,\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n&=b_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots&\ldots\\ a_{n1}x_1+a_{n2}x_2+\ldots+a_{nn}x_n&=b_n. \end{aligned}\right\} \qquad (1)$$

Supposons en outre que le déterminant d des coefficients des inconnues du système (1) (dit encore *déterminant du système*) n'est pas nul. Nous allons montrer qu'avec ces hypothèses le système (1) est toujours compatible et même déterminé.

Au § 2, en résolvant un système de trois équations à trois inconnues nous avons multiplié chaque équation par un facteur convenablement choisi, puis nous avons additionné les équations obtenues. Après quoi, les coefficients de deux des inconnues se sont avérés être nuls. Nous allons montrer maintenant que le facteur en question n'était autre que le cofacteur de l'élément a_{kj} du déterminant du système, a_{kj} étant le coefficient de l'inconnue x_j dans la $k^{\text{ème}}$ équation. Le même procédé sera utilisé pour la résolution du système (1).

Supposons d'abord que le système (1) soit compatible et que $\alpha_1, \alpha_2, \ldots, \alpha_n$ soit une de ses solutions. Ainsi, les identités suivantes sont vérifiées:

$$\left.\begin{aligned} a_{11}\alpha_1+a_{12}\alpha_2+\ldots+a_{1n}\alpha_n&=b_1,\\ a_{21}\alpha_1+a_{22}\alpha_2+\ldots+a_{2n}\alpha_n&=b_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots&\ldots\\ a_{n1}\alpha_1+a_{n2}\alpha_2+\ldots+a_{nn}\alpha_n&=b_n. \end{aligned}\right\} \qquad (2)$$

Soit j un entier, $1 \leqslant j \leqslant n$. Multiplions les deux membres de la première des identités (2) par A_{1j}, c'est-à-dire par le cofacteur de l'élément a_{1j} du déterminant d du système, puis, les deux membres de la seconde des identités (2) par A_{2j}, etc.; finalement, multiplions les deux membres de la dernière des identités (2) par A_{nj}. Additionnant les identités obtenues, il vient

$$\begin{aligned} (a_{11}A_{1j}+a_{21}A_{2j}+\ldots+a_{n1}A_{nj})\alpha_1+&\\ +(a_{12}A_{1j}+a_{22}A_{2j}+\ldots+a_{n2}A_{nj})\,\alpha_2+&\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ +(a_{1j}A_{1j}+a_{2j}A_{2j}+\ldots+a_{nj}A_{nj})\,\alpha_j+&\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ +(a_{1n}A_{1j}+a_{2n}A_{2j}+\ldots+a_{nn}A_{nj})\,\alpha_n=&\\ =b_1A_{1j}+b_2A_{2j}+\ldots+b_nA_{nj}.& \end{aligned}$$

Dans cette égalité, le coefficient de α_j est égal à d, les coefficients des autres α_k $(k \neq j)$ étant nuls en vertu de la remarque faite au

début du paragraphe, tandis que le second membre est égal au déterminant, qui s'obtient du déterminant d en remplaçant sa $j^{\text{ème}}$ colonne par la colonne des seconds membres du système (1). Notant, comme au § 2, ce déterminant par d_j, notre égalité prend la forme

$$d\alpha_j = d_j,$$

d'où

$$\alpha_j = \frac{d_j}{d},$$

car $d \neq 0$.

Ceci prouve que si le système (1) est compatible, il possède alors une solution unique

$$\alpha_1 = \frac{d_1}{d}, \quad \alpha_2 = \frac{d_2}{d}, \ldots, \alpha_n = \frac{d_n}{d}. \tag{3}$$

Maintenant nous allons montrer que la suite des nombres (3) vérifie réellement le système d'équations (1), c'est-à-dire que le système (1) est compatible. Au cours de la démonstration nous allons utiliser les symboles usuels, permettant d'abréger l'écriture.

Toute somme $a_1 + a_2 + \ldots + a_n$ sera notée $\sum\limits_{i=1}^{n} a_i$. Si l'on considère une somme dont les termes sont munis de deux indices, i et j, $i = 1, 2, \ldots, n$, $j = 1, 2, \ldots, m$, on peut former d'abord les sommes $\sum\limits_{j=1}^{m} a_{ij}$, $i = 1, 2, \ldots, n$, et additionner ensuite les sommes obtenues. Pour désigner la somme des éléments a_{ij} nous utiliserons l'écriture

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij}.$$

On aurait pu sommer les a_{ij} par rapport au premier indice et additionner ensuite les sommes obtenues. Ainsi

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m} \sum_{i=1}^{n} a_{ij},$$

autrement dit, *on peut intervertir l'ordre de sommation dans une somme double.*

Remplaçons les inconnues dans la $i^{\text{ème}}$ équation de (1) par leurs valeurs (3). Le premier membre de la $i^{\text{ème}}$ équation étant récrit sous la forme $\sum\limits_{j=1}^{n} a_{ij}x_j$ et compte tenu de la formule $d_j = \sum\limits_{k=1}^{n} b_k A_{kj}$, il vient

$$\sum_{j=1}^{n} a_{ij} \cdot \frac{d_j}{d} = \frac{1}{d} \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{n} b_k A_{kj} \right) = \frac{1}{d} \sum_{k=1}^{n} b_k \left(\sum_{j=1}^{n} a_{ij} A_{kj} \right).$$

Notons que le nombre $\frac{1}{d}$ intervient dans tous les termes, de sorte qu'on peut le mettre en facteur dans la somme ; par ailleurs, après avoir interverti l'ordre de sommation, le nombre b_k est mis en facteur dans la somme par rapport à l'indice j puisque b_k ne dépend pas de j.

Comme on le sait, l'expression $\sum_{j=1}^{n} a_{ij}A_{kj} = a_{i1}A_{k1} + a_{i2}A_{k2} + \ldots + a_{in}A_{kn}$ est égale à d pour $k = i$ et est nulle pour $k \neq i$. Par conséquent, la somme par rapport à l'indice k ne comprend qu'un seul terme, à savoir $b_i d$, c'est-à-dire

$$\sum_{j=1}^{n} a_{ij}\cdot\frac{d_j}{d} = \frac{1}{d}\cdot b_i d = b_i.$$

Ceci prouve que la suite des nombres (3) est réellement la solution du système d'équations (1).

Nous avons obtenu le résultat important suivant:

Un système de n équations linéaires à n inconnues, dont le déterminant est non nul, possède une solution unique. Cette solution est de la forme (3), c'est-à-dire elle s'exprime par les *formules de Cramer*; la formulation de la règle de Cramer est la même que dans le cas d'un système de deux équations (cf. § 2).

Exemple. Résoudre le système d'équations linéaires

$$\left.\begin{aligned} 2x_1 + x_2 - 5x_3 + x_4 &= 8,\\ x_1 - 3x_2 \qquad - 6x_4 &= 9,\\ 2x_2 - x_3 + 2x_4 &= -5,\\ x_1 + 4x_2 - 7x_3 + 6x_4 &= 0. \end{aligned}\right\}$$

Le déterminant

$$d = \begin{vmatrix} 2 & 1 & -5 & 1\\ 1 & -3 & 0 & -6\\ 0 & 2 & -1 & 2\\ 1 & 4 & -7 & 6 \end{vmatrix} = 27$$

de ce système n'étant pas nul, les formules de Cramer donnent la solution. Les valeurs des inconnues auront pour numérateurs les déterminants

$$d_1 = \begin{vmatrix} 8 & 1 & -5 & 1\\ 9 & -3 & 0 & -6\\ -5 & 2 & -1 & 2\\ 0 & 4 & -7 & 6 \end{vmatrix} = 81, \qquad d_2 = \begin{vmatrix} 2 & 8 & -5 & 1\\ 1 & 9 & 0 & -6\\ 0 & -5 & -1 & 2\\ 1 & 0 & -7 & 6 \end{vmatrix} = -108,$$

$$d_3=\begin{vmatrix} 2 & 1 & 8 & 1 \\ 1 & -3 & 9 & -6 \\ 0 & 2 & -5 & 2 \\ 1 & 4 & 0 & 6 \end{vmatrix}=-27, \qquad d_4=\begin{vmatrix} 2 & 1 & -5 & 8 \\ 1 & -3 & 0 & 9 \\ 0 & 2 & -1 & -5 \\ 1 & 4 & -7 & 0 \end{vmatrix}=27.$$

Ainsi

$$x_1=3, \qquad x_2=-4, \qquad x_3=-1, \qquad x_4=1$$

est la solution de notre système ; en outre cette solution est unique.

Nous n'avons pas considéré le cas de systèmes (1) de n équations linéaires à n inconnues à déterminant nul. Ce cas sera étudié au chapitre II, où il sera question de la théorie générale des systèmes d'équations linéaires à un nombre quelconque d'équations et d'inconnues.

Faisons encore une remarque concernant les systèmes de n équations à n inconnues. Soit un système de n équations *homogènes* à n inconnues (cf. § 1):

$$\left.\begin{array}{l} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=0, \\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1+a_{n2}x_2+\ldots+a_{nn}x_n=0. \end{array}\right\} \tag{4}$$

Dans ce cas, chaque déterminant d_j, $j = 1, 2, \ldots, n$, contient une colonne dont tous les éléments sont nuls et, par conséquent, d_j est nul. Ainsi, si le déterminant du système (4) est non nul, c'est-à-dire si les formules de Cramer donnent la solution de (4), celle-ci, qui est dans ce cas unique, est la solution nulle:

$$x_1=0, \ x_2=0, \ \ldots, \ x_n=0. \tag{5}$$

Il en découle le résultat suivant:

Si un système de n équations linéaires homogènes à n inconnues possède des solutions non nulles, alors son déterminant est nul.

La réciproque sera démontrée au § 12, c'est-à-dire on montrera que si le déterminant d'un système homogène est nul, ce système possède alors, en plus de la solution triviale (5), des solutions non nulles.

Exemple. Quelles sont les valeurs du paramètre k pour lesquelles le système d'équations

$$\left.\begin{array}{l} kx_1+x_2=0, \\ x_1+kx_2=0 \end{array}\right\}$$

possède des solutions non nulles ?

Le déterminant de ce système

$$\begin{vmatrix} k & 1 \\ 1 & k \end{vmatrix} = k^2 - 1$$

est nul pour $k = \pm 1$. Il est facile de vérifier que pour chacune de ces valeurs de k, le système possède effectivement des solutions non nulles.

L'importance de la règle de Cramer consiste, d'une manière générale, en ce que, dans les cas où cette règle s'applique, elle donne l'expression explicite de la solution du système, en fonction des coefficients. Néanmoins l'utilisation pratique des formules de Cramer exige des calculs assez laborieux : pour un système de n équations linéaires à n inconnues, on est obligé de calculer $(n + 1)$ déterminants d'ordre n. La méthode d'élimination successive des inconnues, exposée au § 1, est, de ce point de vue, beaucoup plus commode, car les calculs que cette méthode nécessite sont, en substance, équivalents à ceux d'un *seul* déterminant d'ordre n.

Dans les diverses applications on rencontre des systèmes d'équations linéaires dont les coefficients et les seconds membres sont des nombres réels, obtenus à la suite de mesures de certaines grandeurs physiques, c'est-à-dire ils ne sont connus qu'avec une certaine précision. Pour la résolution de tels systèmes la méthode exposée ci-dessus n'est pas toujours valable, car elle donne le résultat avec une erreur assez grande. A ce dessein de nombreuses *méthodes d'itération* ont été élaborées qui permettent de trouver la solution avec une certaine précision à l'aide d'approximations successives. Le lecteur trouvera l'exposé de ce méthodes dans les livres sur la théorie des calculs approchés [1].

---

[1] Voir, par exemple, le livre de A. Karganoff *Méthodes de calcul numérique*, tome I. (*N.d.T.*)

Chapitre II SYSTÈMES D'ÉQUATIONS LINÉAIRES (THÉORIE GÉNÉRALE)

§ 8. Espace vectoriel à n dimensions

Les méthodes que nous avons utilisées avec un tel succès pour la résolution des systèmes cramériens ne suffisent pas pour l'établissement de la théorie générale des systèmes d'équations linéaires. Outre les déterminants et les matrices il nous faudra faire appel à une nouvelle notion, celle d'*espace vectoriel à plusieurs dimensions*, cette notion jouant un rôle encore plus important pour les mathématiques que celles introduites aux paragraphes précédents.

Faisons d'abord quelques remarques. Comme on le sait du cours de géométrie analytique, tout point d'un plan est défini par ses deux coordonnées, les axes de coordonnées étant fixés, c'est-à-dire par un couple ordonné de nombres réels; tout vecteur d'un plan est défini par ses deux composantes, c'est-à-dire encore par un couple ordonné de nombres réels. De même, tout point d'un espace à trois dimensions est bien déterminé par ses trois coordonnées et tout vecteur par ses trois composantes.

Cependant il existe en géométrie, en mécanique et en physique des phénomènes dont la description nécessite fréquemment plus de trois nombres réels. Considérons, par exemple, l'ensemble des boules dans un espace à trois dimensions. Pour qu'une boule soit bien déterminée, il faut se donner les coordonnées de son centre et son rayon, c'est-à-dire un ensemble ordonné de quatre nombres réels, dont le quatrième (le rayon) ne prend que des valeurs positives. Considérons, d'autre part, tous les états possibles d'un corps solide dans un espace à trois dimensions. Pour bien déterminer sa position, il faut les trois coordonnées de son centre de gravité (c'est-à-dire trois nombres réels), la direction d'un axe fixé passant par le centre de gravité (c'est-à-dire deux nombres, deux des trois cosinus directeurs) et, enfin, l'angle de rotation autour de cet axe. Ainsi, un corps solide dans un espace à trois dimensions est bien défini par un ensemble ordonné de six nombres réels.

Ces exemples montrent la nécessité de considérer l'ensemble de tous les n-uples ordonnés de n nombres réels. Cet ensemble muni de la structure algébrique d'addition et de multiplication par un scalaire (ces opérations seront définies ultérieurement de façon

analogue aux opérations correspondantes avec les composantes des vecteurs d'un espace à trois dimensions) est dit espace vectoriel à n dimensions. Ainsi, l'espace vectoriel à n dimensions est une notion purement algébrique, conservant certaines propriétés des plus simples des vecteurs issus de l'origine d'un espace à trois dimensions.

Un ensemble ordonné de n nombres

$$\alpha = (a_1, a_2, \ldots, a_n) \tag{1}$$

est dit *vecteur à n dimensions*. Les nombres a_i, $i = 1, 2, \ldots, n$, sont les *composantes* ou *coordonnées* du vecteur α. Les vecteurs α et

$$\beta = (b_1, b_2, \ldots, b_n) \tag{2}$$

sont *égaux* si et seulement si les composantes de mêmes indices coïncident, c'est-à-dire si $a_i = b_i$ pour tout i, $i = 1, 2, \ldots, n$. Nous désignerons les vecteurs par les lettres grecques minuscules, tandis que les lettres latines minuscules seront utilisées pour noter les nombres.

Voici quelques exemples de vecteurs: 1) Les vecteurs segments de droite issus de l'origine dans un plan ou dans un espace à trois dimensions sont, par rapport à un système d'axes de coordonnées fixé, des vecteurs respectivement à deux ou trois dimensions au sens de la définition précédente. 2) Les coefficients de toute équation linéaire à n inconnues forment un vecteur à n dimensions. 3) Toute solution d'un système d'équations linéaires à n inconnues est un vecteur à n dimensions. 4) Les lignes d'une matrice à s lignes et n colonnes forment s vecteurs à n coordonnées tandis que ses colonnes sont n vecteurs à s coordonnées. 5) La matrice elle-même peut être considérée comme un vecteur à sn composantes: il suffit d'ordonner les éléments de la matrice en disposant les lignes les unes à la suite des autres; en particulier, toute matrice carrée d'ordre n peut être considérée comme un vecteur à n^2 composantes et, réciproquement, tout vecteur à n^2 coordonnées peut être obtenu de cette manière à partir d'une matrice d'ordre n.

Le vecteur

$$\alpha + \beta = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \tag{3}$$

est dit la *somme* des vecteurs (1) et (2); ses composantes sont la somme des coordonnées correspondantes des vecteurs α et β. L'addition des nombres étant commutative et associative, il en est de même des vecteurs.

L'élément nul est le vecteur

$$0 = (0, 0, \ldots, 0). \tag{4}$$

En effet,

$$\alpha+0=(a_1+0,\ a_2+0,\ \ldots,\ a_n+0)=(a_1,\ a_2,\ \ldots,\ a_n)=\alpha.$$

Le nombre nul et le vecteur nul seront notés par le même signe 0; il est toujours facile de comprendre s'il s'agit, selon le contexte, du nombre 0 ou du vecteur nul, de sorte que les confusions sont pratiquement exclues; néanmoins, le lecteur doit prendre en considération que dans les paragraphes suivants le symbole 0 peut avoir ces deux significations.

On appelle vecteur *opposé* au vecteur (1) un vecteur à n dimensions de la forme:

$$-\alpha=(-a_1,\ -a_2,\ \ldots,\ -a_n). \tag{5}$$

Il est clair que $\alpha+(-\alpha)=0$. Maintenant il est facile de voir qu'il existe une opération inverse de l'addition, elle est appelée soustraction des vecteurs (1) et (2) et est définie par la relation $\alpha-\beta=\alpha+(-\beta)$, c'est-à-dire par

$$\alpha-\beta=(a_1-b_1,\ a_2-b_2,\ \ldots,\ a_n-b_n). \tag{6}$$

L'addition des vecteurs à n dimensions, définie par la formule (3), est la généralisation immédiate de la règle géométrique du parallélogramme, qui est valable pour l'addition des vecteurs dans un plan ou dans un espace à trois dimensions. En géométrie, on utilise aussi la multiplication des vecteurs par un nombre réel (ou scalaire): la multiplication d'un vecteur α par un nombre k signifie que le vecteur α a subi, pour $k>0$, une homothétie de rapport k (soit une dilatation pour $k>1$, soit une contraction pour $0<k<1$), et, pour $k<0$, une homothétie de rapport $|k|$ et que son sens a été remplacé par le sens opposé. Cette règle appliquée aux coordonnées d'un vecteur α et étendue au cas des vecteurs à n dimensions nous conduit à la définition suivante:

On appelle *produit d'un vecteur* (1) *par un nombre* k le vecteur $k\alpha$ de composantes:

$$k\alpha=\alpha k=(ka_1,\ ka_2,\ \ldots,\ ka_n). \tag{7}$$

On déduit de cette définition les propriétés importantes, dont la vérification est laissée au lecteur:

$$k(\alpha\pm\beta)=k\alpha\pm k\beta; \tag{8}$$

$$(k\pm l)\alpha=k\alpha\pm l\alpha; \tag{9}$$

$$k(l\alpha)=(kl)\alpha; \tag{10}$$

$$1\cdot\alpha=\alpha. \tag{11}$$

Les relations

$$0\cdot\alpha=0; \tag{12}$$

$$(-1)\cdot\alpha=-\alpha; \tag{13}$$

$$k\cdot 0=0; \tag{14}$$

$$\text{si } k\alpha=0, \quad \text{alors ou} \quad k=0, \text{ ou } \alpha=0, \tag{15}$$

sont également très faciles à vérifier; elles sont des conséquences des propriétés (8) — (11).

L'ensemble de tous les vecteurs à n dimensions de composantes réelles muni des opérations d'addition et de multiplication par un scalaire est appelé *espace vectoriel à n dimensions.*

Il faut noter que la multiplication des vecteurs n'est pas exigée dans la définition des espaces vectoriels à n dimensions. Il ne serait pas difficile de définir une telle opération, en définissant, par exemple, le produit de deux vecteurs α et β comme un vecteur dont les composantes sont les produits des composantes correspondantes de α et β. Néanmoins une telle multiplication trouverait peu d'applications. En effet, comme on le sait, les vecteurs segments de droite issus de l'origine dans un plan ou dans un espace à trois dimensions forment, rapportés à un système d'axes de coordonnées fixé, des espaces vectoriels respectivement à deux et trois dimensions; leur addition et leur multiplication par un scalaire ont un sens géométrique bien défini, tandis que la multiplication de ces vecteurs selon la règle définie ci-dessus n'en a aucun.

Considérons encore un exemple. Le premier membre d'une équation linéaire à n inconnues, c'est-à-dire une expression de la forme

$$f=a_1x_1+a_2x_2+\ldots+a_nx_n,$$

est dit *forme linéaire* des indéterminées $x_1, \ldots, x_n$. La forme linéaire f est bien définie par la donnée du vecteur $(a_1, \ldots, a_n)$ engendré par ses coefficients; réciproquement, tout vecteur à n dimensions définit de façon unique une certaine forme linéaire des indéterminées $x_1, \ldots, x_n$. Par conséquent, l'addition des vecteurs ainsi que leur multiplication par un scalaire définissent les opérations correspondantes sur les formes linéaires; ces opérations ont été beaucoup utilisées au § 1. La multiplication de deux vecteurs définie ci-dessus n'a aucun sens pour les formes linéaires.

§ 9. Dépendance linéaire des vecteurs

Un vecteur β d'un espace vectoriel à n dimensions est dit *proportionnel* à un autre vecteur α s'il existe un nombre k tel que $\beta=k\alpha$ (cf. la formule (7) du paragraphe précédent). En particulier, le vecteur

nul est proportionnel à tout vecteur α, en vertu de l'identité $0 = 0 \cdot \alpha$. Si $\beta = k\alpha$ et $\beta \neq 0$, d'où $k \neq 0$, alors $\alpha = k^{-1}\beta$, c'est-à-dire pour les vecteurs non nuls la propriété d'être proportionnel est symétrique.

Maintenant, nous allons introduire une notion généralisant celle de vecteurs proportionnels (nous avons déjà eu à faire à cette notion au § 4 dans le cas des lignes d'une matrice). Un vecteur β est dit *combinaison linéaire* des vecteurs $\alpha_1, \ldots, \alpha_s$ s'il existe des nombres $l_1, \ldots, l_s$ tels que

$$\beta = l_1\alpha_1 + l_2\alpha_2 + \ldots + l_s\alpha_s.$$

Ainsi, la $j^{\text{ème}}$ composante du vecteur β, $j = 1, 2, \ldots, n$, en vertu de la définition de la somme des vecteurs et du produit d'un vecteur par un scalaire, est égale à la somme des $j^{\text{èmes}}$ composantes des vecteurs $\alpha_1, \ldots, \alpha_s$, multipliées respectivement par les nombres $l_1, \ldots, l_s$.

Les vecteurs

$$\alpha_1, \alpha_2, \ldots, \alpha_{r-1}, \alpha_r \qquad (r \geqslant 2) \tag{1}$$

sont dits *linéairement dépendants* si l'un au moins de ces vecteurs est une combinaison linéaire des autres vecteurs de l'ensemble (1). Dans le cas contraire les vecteurs (1) sont dits *linéairement indépendants*. Un ensemble de vecteurs linéairement dépendants (resp. indépendants) s'appelle parfois système ou famille non libre (resp. libre).

Cette définition importante peut encore être énoncée de façon suivante: on dit que les vecteurs (1) sont linéairement dépendants s'il existe des nombres $k_1, \ldots, k_r$ *non tous nuls*, tels que

$$k_1\alpha_1 + k_2\alpha_2 + \ldots + k_r\alpha_r = 0. \tag{2}$$

Il n'y a aucune difficulté à montrer l'équivalence de ces définitions. Supposons, par exemple, que le vecteur α_r de l'ensemble (1) soit une combinaison linéaire des autres vecteurs de (1):

$$\alpha_r = l_1\alpha_1 + l_2\alpha_2 + \ldots + l_{r-1}\alpha_{r-1}.$$

Ceci entraîne l'égalité

$$l_1\alpha_1 + l_2\alpha_2 + \ldots + l_{r-1}\alpha_{r-1} - \alpha_r = 0,$$

c'est-à-dire une relation de la forme (2) avec $k_i = l_i$, $i = 1, 2, \ldots, r-1$ et $k_r = -1$, $k_r \neq 0$. Inversement, supposons que les vecteurs (1) vérifient une relation de la forme (2) avec, par exemple, $k_r \neq 0$. Alors

$$\alpha_r = \left(-\frac{k_1}{k_r}\right)\alpha_1 + \left(-\frac{k_2}{k_r}\right)\alpha_2 + \ldots + \left(-\frac{k_{r-1}}{k_r}\right)\alpha_{r-1},$$

c'est-à-dire le vecteur α_r est une combinaison linéaire des vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_{r-1}$.

Exemple. Les vecteurs

$$\alpha_1=(5,\ 2,\ 1),\quad \alpha_2=(-1,\ 3,\ 3),\quad \alpha_3=(9,\ 7,\ 5),\quad \alpha_4=(3,\ 8,\ 7)$$

sont linéairement dépendants car ils vérifient la relation

$$4\alpha_1-\alpha_2-3\alpha_3+2\alpha_4=0.$$

Dans cette relation tous les coefficients sont non nuls. Il existe néanmoins d'autres relations linéaires entre les vecteurs donnés avec des coefficients qui ne sont pas tous nuls, comme le montrent les deux égalités suivantes

$$2\alpha_1+\alpha_2-\alpha_3=0,\quad 3\alpha_2+\alpha_3-2\alpha_4=0.$$

La seconde définition de la dépendance linéaire est également valable pour $r = 1$, c'est-à-dire pour un ensemble composé d'un vecteur α: *cet ensemble sera linéairement dépendant si et seulement si* $\alpha = 0$. En effet, si $\alpha = 0$, alors $k\alpha = 0$ pour $k = 1$. Inversement, si $k\alpha = 0$ et $k \neq 0$, alors $\alpha = 0$.

Il faut noter une propriété de la notion d'ensemble de vecteurs linéairement dépendants.

Si un sous-ensemble d'un ensemble (1) *est constitué de vecteurs linéairement dépendants, alors l'ensemble* (1) *l'est aussi.*

En effet, soient les vecteurs $\alpha_1, \ldots, \alpha_s$ de l'ensemble (1), où $s < r$, liés par la relation

$$k_1\alpha_1+k_2\alpha_2+\ldots+k_s\alpha_s=0,$$

avec les coefficients k_j, $j = 1, 2, \ldots, s$, non tous nuls. On en déduit la relation

$$k_1\alpha_1+k_2\alpha_2+\ldots+k_s\alpha_s+0\cdot\alpha_{s+1}+\ldots+0\cdot\alpha_r=0,$$

autrement dit, l'ensemble (1) est constitué de vecteurs linéairement dépendants.

Il découle de cette propriété que *tout ensemble de deux vecteurs identiques ou, en général, de deux vecteurs proportionnels ainsi que tout ensemble contenant le vecteur nul sont des familles non libres.* Notons que la propriété que nous venons de démontrer peut être encore énoncée de la manière suivante: *si les vecteurs* (1) *sont linéairement indépendants, alors tous les vecteurs d'un sous-ensemble quelconque de* (1) *le sont aussi.*

La question suivante se pose: combien de vecteurs peut contenir une famille libre de vecteurs à n dimensions et, en particulier, existe-t-il de familles libres contenant un nombre arbitrairement grand de vecteurs? Pour répondre à cette question considérons dans un espace vectoriel à n dimensions l'ensemble de vecteurs à n dimensions

suivant

$$\left.\begin{aligned} \varepsilon_1 &= (1,\ 0,\ 0,\ \ldots,\ 0), \\ \varepsilon_2 &= (0,\ 1,\ 0,\ \ldots,\ 0), \\ &\ldots\ldots\ldots\ldots \\ \varepsilon_n &= (0,\ 0,\ 0,\ \ldots,\ 1), \end{aligned}\right\} \qquad (3)$$

qu'on appelle *vecteurs unités* de cet espace. *Les vecteurs unités sont linéairement indépendants.* En effet, supposons que

$$k_1\varepsilon_1 + k_2\varepsilon_2 + \ldots + k_n\varepsilon_n = 0\,;$$

puisque le premier membre de cette relation est le vecteur $(k_1,\ k_2,\ \ldots,\ k_n)$, il vient

$$(k_1,\ k_2,\ \ldots,\ k_n) = 0,$$

c'est-à-dire $k_i = 0$ pour $i = 1,\ 2,\ \ldots,\ n$.

Ainsi, nous avons trouvé dans un espace vectoriel à n dimensions un système de n vecteurs linéairement indépendants. Le lecteur verra plus loin qu'il y existe une infinité de différentes familles libres.

D'autre part, démontrons le théorème suivant:

Toute famille de s vecteurs d'un espace vectoriel à n dimensions est non libre si $s > n$.

En effet, soient

$$\begin{aligned} \alpha_1 &= (a_{11},\ a_{12},\ \ldots,\ a_{1n}), \\ \alpha_2 &= (a_{21},\ a_{22},\ \ldots,\ a_{2n}), \\ &\ldots\ldots\ldots\ldots \\ \alpha_s &= (a_{s1},\ a_{s2},\ \ldots,\ a_{sn}) \end{aligned}$$

les vecteurs donnés. On doit trouver des nombres $k_1,\ k_2,\ \ldots,\ k_s$ non tous nuls de façon que

$$k_1\alpha_1 + k_2\alpha_2 + \ldots + k_s\alpha_s = 0. \qquad (4)$$

Passons de cette égalité aux égalités correspondantes pour les coordonnées des vecteurs; il vient

$$\left.\begin{aligned} a_{11}k_1 + a_{21}k_2 + \ldots + a_{s1}k_s &= 0, \\ a_{12}k_1 + a_{22}k_2 + \ldots + a_{s2}k_s &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}k_1 + a_{2n}k_2 + \ldots + a_{sn}k_s &= 0. \end{aligned}\right\} \qquad (5)$$

Or, les égalités (5) forment un système de n équations linéaires homogènes à s inconnues $k_1,\ k_2,\ \ldots,\ k_s$. Le nombre des inconnues étant supérieur à celui des équations, le résultat correspondant

du § 1 montre que le système (5) possède des solutions non nulles. Par conséquent, on peut choisir des nombres $k_1, k_2, \ldots, k_s$ non tous nuls qui satisfont à (4). Le théorème est ainsi démontré.

Une famille libre de vecteurs à n dimensions

$$\alpha_1, \alpha_2, \ldots, \alpha_r \qquad (6)$$

est dite *maximale* si la famille $\alpha_1, \ldots, \alpha_r, \beta$ est non libre quel que soit le vecteur β à n dimensions. Toute relation linéaire entre les vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta$ devant contenir β avec un coefficient non nul (dans le cas contraire, la famille (6) serait non libre), le vecteur β est donc une combinaison linéaire des vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_r$. Par conséquent, la famille (6) ne peut être maximale que lorsqu'elle est libre et tout vecteur β à n dimensions est une combinaison linéaire des vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_r$.

Il découle des résultats obtenus ci-dessus que *toute famille libre de n vecteurs dans un espace à n dimensions est toujours maximale, de même qu'une famille maximale de cet espace ne peut pas contenir plus de n vecteurs.*

Quelle que soit la famille libre de vecteurs à n dimensions, on peut toujours trouver une famille maximale qui la contient. En effet, si la famille donnée n'est pas maximale, on peut y ajouter un vecteur de manière que la famille ainsi obtenue soit libre. Si cette dernière n'est pas maximale, on peut y ajouter encore un vecteur et ainsi de suite. Ce processus doit s'arrêter car toute famille de $(n + 1)$ vecteurs à n dimensions est non libre.

Toute famille composée d'un vecteur non nul étant libre, il en résulte que *tout vecteur non nul appartient à une certaine famille maximale*; par conséquent, *il existe une infinité de différentes familles maximales dans un espace à n dimensions.*

Il est naturel de se demander s'il existe dans un espace à n dimensions des familles maximales contenant moins de n vecteurs, ou bien le nombre des vecteurs de telles familles est toujours égal à n. La réponse à cette question importante sera donnée un peu plus bas, après quelques considérations préliminaires.

Si un vecteur β est une combinaison linéaire des vecteurs

$$\alpha_1, \alpha_2, \ldots, \alpha_r, \qquad (7)$$

on dit souvent que β *s'exprime linéairement par les vecteurs* (7). Evidemment, si un vecteur β s'exprime linéairement par les vecteurs formant une sous-famille de la famille (7), alors il s'exprime linéairement par tous les vecteurs (7): il suffit d'ajouter à la combinaison linéaire donnant β les autres vecteurs de la famille (7) avec des coefficients nuls. Plus généralement, on dit que les *vecteurs d'une famille donnée*

$$\beta_1, \beta_2, \ldots, \beta_s \qquad (8)$$

s'expriment linéairement par les vecteurs de la famille (7) si tout vecteur β_i, $i = 1, 2, \ldots, s$, est une combinaison linéaire des vecteurs (7).

Nous allons démontrer que cette notion est transitive, autrement dit, *si les vecteurs de la famille* (8) *s'expriment linéairement par les vecteurs de la famille* (7) *et si les vecteurs*

$$\gamma_1, \gamma_2, \ldots, \gamma_t \tag{9}$$

s'expriment linéairement par les vecteurs (8), *alors les vecteurs* (9) *s'expriment linéairement par ceux de la famille* (7).

En effet,

$$\gamma_j = \sum_{i=1}^{s} l_{ji}\beta_i, \qquad j = 1, 2, \ldots, t, \tag{10}$$

avec $\beta_i = \sum_{m=1}^{r} k_{im}\alpha_m$, $i = 1, 2, \ldots, s$. Substituant ces expressions dans (10), il vient

$$\gamma_j = \sum_{i=1}^{s} l_{ji} \left(\sum_{m=1}^{r} k_{im}\alpha_m\right) =$$

$$= \sum_{m=1}^{r} \left(\sum_{i=1}^{s} l_{ji}k_{im}\right) \alpha_m,$$

autrement dit, tout vecteur γ_j, pour $j = 1, 2, \ldots, t$, est une combinaison linéaire des vecteurs (7).

Deux ensembles de vecteurs sont dits *équivalents* si leurs vecteurs s'expriment linéairement les uns par les autres. La propriété de transitivité que nous venons de démontrer montre que l'équivalence de deux ensembles de vecteurs est une propriété transitive; il en résulte aussi la proposition suivante: un vecteur qui s'exprime linéairement par les vecteurs d'un ensemble donné est également une combinaison linéaire des vecteurs de tout autre ensemble équivalent.

Si un ensemble de vecteurs donné est équivalent à une famille libre, alors cet ensemble n'est pas forcément une famille libre. Mais si les deux ensembles de vecteurs sont équivalents et sont en même temps des familles libres, on peut en déduire une conclusion importante sur le nombre des vecteurs appartenant à ces deux ensembles. Démontrons d'abord le théorème suivant que nous appellerons désormais, vu son importance (et pour la commodité des références), *théorème fondamental.*

Soient dans un espace vectoriel à n dimensions deux familles de vecteurs équivalentes:

(I) $\alpha_1, \alpha_2, \ldots, \alpha_r$,

(II) $\beta_1, \beta_2, \ldots, \beta_s$.

Si la première famille est libre, alors le nombre de ses vecteurs n'est pas supérieur à celui des vecteurs de la seconde famille, c'est-à-dire $r \leqslant s$.

Supposons que $r > s$. En vertu des hypothèses du théorème, tout vecteur de (I) est une combinaison linéaire des vecteurs de l'ensemble (II):

$$\left.\begin{aligned} \alpha_1 &= a_{11}\beta_1 + a_{12}\beta_2 + \ldots + a_{1s}\beta_s, \\ \alpha_2 &= a_{21}\beta_1 + a_{22}\beta_2 + \ldots + a_{2s}\beta_s, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_r &= a_{r1}\beta_1 + a_{r2}\beta_2 + \ldots + a_{rs}\beta_s. \end{aligned}\right\} \tag{11}$$

Les coefficients de ces relations linéaires forment un système de r vecteurs à s dimensions:

$$\begin{aligned} \gamma_1 &= (a_{11}, a_{12}, \ldots, a_{1s}), \\ \gamma_2 &= (a_{21}, a_{22}, \ldots, a_{2s}), \\ &\ldots\ldots\ldots\ldots \\ \gamma_r &= (a_{r1}, a_{r2}, \ldots, a_{rs}). \end{aligned}$$

Comme $r > s$, les vecteurs γ_j, $j = 1, 2, \ldots, r$, sont linéairement dépendants:

$$k_1\gamma_1 + k_2\gamma_2 + \ldots + k_r\gamma_r = 0,$$

les coefficients $k_1, k_2, \ldots, k_r$ n'étant pas tous nuls. Cela nous conduit aux égalités correspondantes pour les composantes:

$$\sum_{i=1}^{r} k_i a_{ij} = 0, \qquad j = 1, 2, \ldots, s. \tag{12}$$

Formons maintenant la combinaison linéaire des vecteurs de l'ensemble (I) avec les coefficients k_j:

$$k_1\alpha_1 + k_2\alpha_2 + \ldots + k_r\alpha_r = \sum_{i=1}^{r} k_i\alpha_i.$$

Utilisant (11) et (12), il vient:

$$\sum_{i=1}^{r} k_i\alpha_i = \sum_{i=1}^{r} k_i \Big(\sum_{j=1}^{s} a_{ij}\beta_j\Big) = \sum_{j=1}^{s} \Big(\sum_{i=1}^{r} k_i a_{ij}\Big)\beta_j = 0,$$

ce qui est en contradiction avec l'hypothèse du théorème d'après laquelle les vecteurs de l'ensemble (I) sont linéairement indépendants.

On déduit du théorème fondamental démontré ci-dessus la proposition suivante:

Deux familles libres équivalentes contiennent le même nombre de vecteurs.

Deux familles maximales dans un espace à n dimensions sont manifestement équivalentes. Par conséquent, elles contiennent le même nombre de vecteurs et, comme il existe des familles maximales comprenant exactement n vecteurs à n dimensions, il en résulte que *toute famille maximale, dans un espace à n dimensions, contient n vecteurs.* C'est la réponse à la question posée ci-dessus.

Bien d'autres corollaires découlent des résultats obtenus.

Quelle que soit la manière dont on choisit dans une famille non libre une sous-famille maximale, le nombre de vecteurs formant cette sous-famille ne varie pas.

En effet, si dans une famille de vecteurs

$$\alpha_1, \alpha_2, \ldots, \alpha_r \tag{13}$$

la sous-famille

$$\alpha_1, \alpha_2, \ldots, \alpha_s, \qquad s < r, \tag{14}$$

est maximale, alors chaque vecteur α_j, $j = s + 1, \ldots, r$, est une combinaison linéaire des vecteurs (14). D'autre part, tout vecteur α_j de la famille (13) s'exprime linéairement par les vecteurs de cette famille ; il suffit pour cela de prendre α_j avec le coefficient 1 et les autres vecteurs de la famille (13) avec les coefficients nuls. A présent, il est facile de voir que les familles (13) et (14) sont équivalentes. Il en résulte que la famille (13) est équivalente à toutes ses sous-familles maximales, de sorte que toutes ses sous-familles maximales sont équivalentes. Mais comme elles sont, en même temps, libres, il en résulte immédiatement qu'elles contiennent le même nombre de vecteurs.

Le nombre de vecteurs d'une sous-famille maximale quelconque d'un ensemble de vecteurs donné est appelé *rang* de ce dernier. Utilisant cette notion nous allons maintenant déduire encore une conséquence du théorème fondamental.

Soient deux ensembles de vecteurs à n dimensions

$$\alpha_1, \alpha_2, \ldots, \alpha_r, \tag{15}$$

$$\beta_1, \beta_2, \ldots, \beta_s \tag{16}$$

(pas forcément linéairement indépendants) respectivement de rang k et l. Si les vecteurs du premier ensemble s'expriment linéairement en fonction des vecteurs du second, alors $k \leqslant l$. Si ces ensembles sont équivalents, alors $k = l$.

En effet, soient

$$\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k} \tag{17}$$

et

$$\beta_{j_1}, \beta_{j_2}, \ldots, \beta_{j_l} \tag{18}$$

deux sous-familles maximales extraites respectivement des ensembles (15) et (16). Alors les ensembles (15) et (17) sont équivalents et il en est de même pour les familles (16) et (18). Les vecteurs (15) s'exprimant linéairement par les vecteurs (16), il en résulte que les vecteurs (17) s'expriment linéairement par les vecteurs de l'ensemble (16) et, par conséquent, par les vecteurs de la famille équivalente (18). Vu l'indépendance linéaire des vecteurs de la famille (17), il ne reste donc qu'à appliquer le théorème fondamental. La seconde partie de notre proposition est une conséquence directe de la première.

§ 10. Rang d'une matrice

Soit un ensemble de vecteurs à n dimensions; il est naturel de se poser la question: est-ce que cet ensemble est une famille libre ou non libre? On ne peut pas s'attendre à ce que, dans chaque cas concret, la réponse à cette question puisse être obtenue sans difficulté. Par exemple, un examen superficiel ne permet pas d'établir des relations linéaires entre les vecteurs

$$\alpha = (2, -5, 1, -1), \quad \beta = (1, 3, 6, 5), \quad \gamma = (-1, 4, 1, 2),$$

bien qu'il en existe une de la forme

$$7\alpha - 3\beta + 11\gamma = 0.$$

Le § 1 donne une des méthodes permettant de répondre à cette question. Les composantes des vecteurs étant supposées connues, on obtient un système d'équations linéaires homogènes par rapport aux coefficients de la relation linéaire entre les vecteurs donnés, ce système d'équations pouvant être résolu par la méthode de Gauss. Dans ce paragraphe nous donnerons une autre approche du problème considéré; en même temps cela nous permettra d'atteindre notre but fondamental: trouver une méthode de résolution des systèmes arbitraires d'équations linéaires.

Soit une matrice

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{s1} & a_{s2} & \dots & a_{sn} \end{pmatrix}$$

à s lignes et n colonnes, les entiers s et n sont arbitraires. Les colonnes de la matrice A, interprétées comme des vecteurs à s dimensions, peuvent être linéairement dépendantes. Le rang du système des colonnes de A, c'est-à-dire le nombre maximal de colonnes de la matrice A linéairement indépendantes (plus précisément, le nombre de colonnes formant une sous-famille maximale quelconque du système des colonnes de A), est appelé *rang* de la matrice A.

Il est clair que l'on peut considérer de la même manière les lignes d'une matrice A comme des vecteurs à n dimensions. Comme on le verra plus bas, le rang du système des lignes d'une matrice A est égal à celui du système de ses colonnes, c'est-à-dire au rang de la matrice A. La démonstration de cette proposition inattendue sera donnée après l'introduction d'une autre définition du rang d'une matrice, qui donne en même temps un procédé pratique de son calcul.

Nous allons d'abord généraliser la notion de mineur pour des matrices rectangulaires. Fixons k lignes et k colonnes quelconques d'une matrice A, où $k \leqslant \min(s, n)$. Les éléments se trouvant à l'intersection des lignes et des colonnes fixées forment une matrice carrée d'ordre k, dont le déterminant est dit *mineur d'ordre k* de la matrice A. Ce sont les ordres des mineurs non nuls de la matrice A qui nous intéressent particulièrement et, surtout, l'*ordre le plus élevé* de ces mineurs. Pour trouver l'ordre le plus élevé des mineurs non nuls, il est utile de prendre en considération la remarque suivante: *si tous les mineurs d'ordre k de la matrice A sont nuls, alors tous les mineurs d'ordre supérieur à k de cette matrice s'annulent également.* En effet, d'après le théorème de Laplace, développant chaque mineur d'ordre $k+j$, $k < k+j \leqslant \min(s, n)$ par rapport aux mineurs extraits des k lignes quelconques d'une matrice A, nous mettons ce mineur sous la forme d'une somme de plusieurs mineurs d'ordre k, multipliés chacun par un certain mineur d'ordre j, ce qui prouve notre proposition.

A présent, démontrons le *théorème suivant sur le rang d'une matrice*:

L'ordre le plus élevé des mineurs non nuls d'une matrice A est égal au rang de A.

Démonstration. Soit r l'ordre le plus élevé des mineurs non nuls de la matrice A. On peut supposer, sans restreindre la généralité, que le mineur D d'ordre r, se trouvant à l'intersection des r premières lignes et des r premières colonnes de A,

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1r} & a_{1,r+1} & \ldots & a_{1n} \\ \ldots & D & \ldots & \ldots & \ldots & \ldots \\ a_{r1} & \ldots & a_{rr} & a_{r,r+1} & \ldots & a_{rn} \\ a_{r+1,1} & \ldots & a_{r+1,r} & a_{r+1,r+1} & \ldots & a_{r+1,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{s1} & \ldots & a_{sr} & a_{s,r+1} & \ldots & a_{sn} \end{pmatrix},$$

n'est pas nul, $D \neq 0$. Alors les r premières colonnes de A sont linéairement indépendantes. En effet, s'il existait une relation linéaire entre ces colonnes, alors les colonnes du mineur D seraient

également linéairement dépendantes de sorte que D serait nul, car l'addition des vecteurs est équivalente à celle de leurs composantes.

Montrons maintenant que toute colonne de la matrice A d'indice l avec $r < l \leqslant n$ est une combinaison linéaire des r premières colonnes de A. Pour i quelconque, $1 \leqslant i \leqslant s$, formons le mineur auxiliaire Δ_i d'ordre $(r+1)$

$$\Delta_i = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1l} \\ \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{rl} \\ a_{i1} & \dots & a_{ir} & a_{il} \end{vmatrix}.$$

Δ_i s'obtient de D en le complétant de la $l^{\text{ème}}$ colonne et de la $i^{\text{ème}}$ ligne de la matrice A. Le mineur Δ_i est nul pour tout indice i. En effet, si $i > r$, alors Δ_i est un mineur d'ordre $(r+1)$ de la matrice A et, par conséquent, est nul, en vertu du choix de l'entier r. Si, par contre, $i \leqslant r$, alors Δ_i n'est plus un mineur de la matrice A, car il ne peut pas être obtenu en supprimant un certain nombre de lignes et de colonnes de A; néanmoins, dans ce cas Δ_i s'annule, car il contient deux lignes identiques.

Considérons les cofacteurs des éléments de la dernière ligne dans le déterminant Δ_i. Il est clair que le mineur D est le cofacteur de a_{il} dans Δ_i. Le cofacteur de l'élément a_{ij} dans Δ_i, pour $1 \leqslant j \leqslant r$, est le nombre

$$A_j = (-1)^{(r+1)+j} \begin{vmatrix} a_{11} & \dots & a_{1,\,j-1} & a_{1,\,j+1} & \dots & a_{1r} & a_{1l} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{r,\,j-1} & a_{r,\,j+1} & \dots & a_{rr} & a_{rl} \end{vmatrix},$$

ce nombre ne dépendant pas de i, notons-le donc par A_j. Développant le déterminant Δ_i par rapport aux éléments de sa dernière ligne, nous obtenons, vu que $\Delta_i = 0$,

$$a_{i1}A_1 + a_{i2}A_2 + \dots + a_{ir}A_r + a_{il}D = 0,$$

ou, encore, vu que $D \neq 0$,

$$a_{il} = -\frac{A_1}{D} a_{i1} - \frac{A_2}{D} a_{i2} - \dots - \frac{A_r}{D} a_{ir}.$$

Cette égalité est valable pour tout i, $i = 1, 2, \dots, s$; les coefficients $-\frac{A_j}{D}$ ne dépendant pas de i, il en résulte donc que la $l^{\text{ème}}$ colonne est une combinaison linéaire des r premières colonnes de la matrice A, les coefficients de la combinaison linéaire étant, respectivement, $-\frac{A_1}{D}, -\frac{A_2}{D}, \dots, -\frac{A_r}{D}$.

Ainsi, nous avons trouvé parmi les colonnes de la matrice A une sous-famille maximale contenant exactement r colonnes. Ceci démontre que le rang de A est égal à r. Le théorème sur le rang d'une matrice est démontré.

Ce théorème donne une méthode pratique de calcul du rang d'une matrice et, par conséquent, permet de répondre à la question posée au début du paragraphe: une famille de vecteurs donnée est-elle libre ou non libre? Formant la matrice dont les colonnes sont les vecteurs donnés et calculant son rang, on trouve le nombre maximal de vecteurs linéairement indépendants de l'ensemble en question.

La méthode de calcul du rang d'une matrice, basée sur le théorème du rang, nécessite, généralement, le calcul d'un nombre assez élevé, quoique fini, de mineurs. Une remarque permet, cependant, de simplifier considérablement ces calculs. Si le lecteur veut se donner la peine de revoir la démonstration du théorème du rang, il constatera que dans nos raisonnements nous n'avons pas tenu compte de ce que *tous* les mineurs d'ordre $(r + 1)$ étaient nuls, mais seulement de ce que les mineurs d'ordre $(r + 1)$, obtenus du mineur D non nul d'ordre r en le complétant d'une ligne et d'une colonne, étaient tous nuls (tous ces mineurs d'ordre $(r + 1)$ contiennent le mineur D). Cela était suffisant pour en déduire que le nombre maximal de colonnes linéairement indépendantes d'une matrice A était égal à r, ce qui entraîne que tous les mineurs d'ordre $(r + 1)$ de A sont nuls. Nous sommes conduits à la *règle* suivante *de calcul du rang d'une matrice*:

Pour calculer le rang d'une matrice, il faut passer des mineurs d'ordres inférieurs à ceux d'ordres plus élevés. Un mineur D d'ordre k non nul une fois trouvé, il suffit de calculer les mineurs d'ordre $(k + 1)$ contenant le mineur D. Si tous ces mineurs d'ordre $(k + 1)$ sont nuls, alors le rang de la matrice est k.

Exemples.

1. Calculer le rang de la matrice

$$A = \begin{pmatrix} 2 & -4 & 3 & 1 & 0 \\ 1 & -2 & 1 & -4 & 2 \\ 0 & 1 & -1 & 3 & 1 \\ 4 & -7 & 4 & -4 & 5 \end{pmatrix}.$$

Le mineur d'ordre 2, se trouvant à l'intersection des deux premières lignes et des deux premières colonnes de A, est nul. Néanmoins, la matrice A possède des mineurs d'ordre 2 non nuls, par exemple,

$$d = \begin{vmatrix} -4 & 3 \\ -2 & 1 \end{vmatrix} \neq 0.$$

Le mineur d'ordre 3

$$d'=\begin{vmatrix}2 & -4 & 3\\ 1 & -2 & 1\\ 0 & 1 & -1\end{vmatrix},$$

encadrant le mineur d est non nul: $d'=1$. Par contre, les deux mineurs d'ordre 4, qui contiennent d', sont nuls:

$$\begin{vmatrix}2 & -4 & 3 & 1\\ 1 & -2 & 1 & -4\\ 0 & 1 & -1 & 3\\ 4 & -7 & 4 & -4\end{vmatrix}=0,\quad \begin{vmatrix}2 & -4 & 3 & 0\\ 1 & -2 & 1 & 2\\ 0 & 1 & -1 & 1\\ 4 & -7 & 4 & 5\end{vmatrix}=0.$$

Ainsi, le rang de la matrice A est trois.

2. Trouver une sous-famille maximale dans l'ensemble de vecteurs

$$\alpha_1=(2,\ -2,\ -4),\quad \alpha_2=(1,\ 9,\ 3),\quad \alpha_3=(-2,\ -4,\ 1),\quad \alpha_4=(3,\ 7,\ -1).$$

Formons la matrice

$$\begin{pmatrix}2 & 1 & -2 & 3\\ -2 & 9 & -4 & 7\\ -4 & 3 & 1 & -1\end{pmatrix}$$

qui a pour colonnes les vecteurs donnés. Le rang de cette matrice est deux car le mineur D d'ordre 2 se trouvant à l'intersection des deux premières lignes et des deux premières colonnes de la matrice est non nul et tous les mineurs d'ordre 3 contenant D sont nuls. Il s'ensuit que les vecteurs α_1 et α_2 forment une des sous-familles maximales de l'ensemble donné.

La proposition suivante (déjà énoncée précédemment) est un corollaire du théorème sur le rang d'une matrice:

Le nombre maximal de lignes linéairement indépendantes dans une matrice est égal au nombre maximal de ses colonnes linéairement indépendantes, c'est-à-dire au rang de la matrice.

Pour prouver cette proposition considérons la transposée de la matrice donnée, c'est-à-dire la matrice dont les lignes sont les colonnes de la matrice initiale disposées selon le même ordre. L'ordre le plus élevé des mineurs non nuls de la matrice transposée est, manifestement, le même que celui de la matrice initiale, car la transposition d'une matrice ne change pas les déterminants et, de plus, pour tout mineur de la matrice initiale, le mineur transposé se trouve parmi les mineurs de la matrice transposée et inversement. Il en résulte que le rang de la matrice transposée est égal à celui de la matrice donnée; or, le rang de la matrice transposée est égal au nombre maximal de colonnes linéairement indépendantes de cette matrice, à savoir au nombre maximal de *lignes* linéairement indépendantes de la matrice initiale.

Exemple. Nous avons déjà introduit au § 8 les formes linéaires de n indéterminées et défini leur addition, ainsi que la multiplication des formes par un scalaire. Cette définition permet d'étendre aux formes linéaires de n indéterminées la notion d'indépendance linéaire ainsi que tous les résultats qui s'y rattachent.

Soit un ensemble de formes linéaires

$$f_1 = x_1 + 2x_2 + x_3 + 3x_4,$$
$$f_2 = 4x_1 - x_2 - 5x_3 - 6x_4,$$
$$f_3 = x_1 - 3x_2 - 4x_3 - 7x_4,$$
$$f_4 = 2x_1 + x_2 - x_3.$$

Il faut en indiquer une sous-famille maximale.

Formons la matrice des coefficients des formes

$$\begin{pmatrix} 1 & 2 & 1 & 3 \\ 4 & -1 & -5 & -6 \\ 1 & -3 & -4 & -7 \\ 2 & 1 & -1 & 0 \end{pmatrix}$$

et calculons le rang de cette matrice. Comme il est facile de le vérifier, le mineur D d'ordre 2 se trouvant à l'intersection des deux premières lignes et des deux premières colonnes n'est pas nul, par contre tous les mineurs d'ordre 3 qui contiennent D sont nuls. Il en découle que les deux premières lignes de notre matrice sont linéairement indépendantes, tandis que la troisième et la quatrième ligne sont des combinaisons linéaires des deux premières. Donc, les formes f_1 et f_2 forment une sous-famille maximale dans l'ensemble des formes linéaires données.

Indiquons encore un corollaire important du théorème sur le rang d'une matrice:

Pour qu'un déterminant d'ordre n soit nul, il faut et il suffit qu'il existe une dépendance linéaire entre ses lignes.

La propriété 8, démontrée au § 4, montre la suffisance de cette condition. Montrons sa nécessité. Supposons qu'un déterminant d'ordre n soit nul, autrement dit, soit une matrice carrée d'ordre n dont le seul mineur d'ordre n est nul. Il en résulte que l'ordre le plus élevé des mineurs non nuls de cette matrice est strictement inférieur à n, c'est-à-dire le rang de la matrice est inférieur à n; en vertu de la proposition correspondante, démontrée ci-dessus, les lignes de cette matrice sont linéairement dépendantes. Bien entendu, dans l'énoncé de ce corollaire nous aurions pu remplacer les lignes par les colonnes.

Il existe encore une méthode de calcul du rang d'une matrice, qui n'a pas recours au théorème sur le rang d'une matrice et qui n'exige pas le calcul de déterminants. Mais cette méthode n'est valable que lorsque nous voulons calculer le rang lui-même et ne sommes pas intéressés à savoir quelles colonnes (ou lignes) de la matrice donnée forment une sous-famille maximale. Exposons cette méthode.

On appelle *transformations élémentaires* d'une matrice A les transformations suivantes.

(a) permutation de deux lignes (ou colonnes);
(b) multiplication d'une ligne (ou colonne) par un nombre non nul;
(c) addition d'une ligne (ou colonne) multipliée par un nombre quelconque à une autre ligne (ou colonne).

Il est facile de vérifier que les *transformations élémentaires conservent le rang d'une matrice*. En effet, si nous les appliquons, par exemple, aux colonnes, le système des colonnes d'une matrice, à la suite de ces transformations, est remplacé par un système équivalent. Montrons cette proposition seulement pour la transformation (c), car elle est évidente pour (a) et (b). Supposons que la $j^{\text{ème}}$ colonne multipliée par un nombre k soit ajoutée à la $i^{\text{ème}}$ colonne. Notant les vecteurs colonnes de la matrice initiale par

$$\alpha_1, \ldots, \alpha_i, \ldots, \alpha_j, \ldots, \alpha_n, \tag{1}$$

après la transformation (c) ces colonnes deviennent

$$\alpha_1, \ldots, \alpha_i' = \alpha_i + k\alpha_j, \ldots, \alpha_j, \ldots, \alpha_n. \tag{2}$$

Les vecteurs de l'ensemble (2) s'expriment linéairement par les vecteurs de l'ensemble (1) et inversement, comme le montrent les formules:

$$\alpha_i = \alpha_i' - k\alpha_j.$$

Donc, ces ensembles sont équivalents et, par conséquent, leurs sous-familles maximales contiennent toutes le même nombre de vecteurs.

Ainsi, pour calculer le rang d'une matrice on peut d'abord la simplifier par une série de transformations élémentaires.

Une matrice à s lignes et n colonnes est dite *diagonale* si tous ses éléments a_{ij} sont nuls, excepté les éléments $a_{11}, a_{22}, \ldots, a_{rr}$ $(0 \leqslant r \leqslant \min(s, n))$, égaux à l'unité. Il est clair que le rang d'une telle matrice est r.

Toute matrice peut être réduite à la forme diagonale par des transformations élémentaires.

En effet, soit une matrice

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \cdot & \cdot \; \cdot & \cdot \\ a_{s1} & \ldots & a_{sn} \end{pmatrix}.$$

Si tous ses éléments sont nuls, alors elle a déjà la forme diagonale. Supposons donc que cette matrice possède des éléments non nuls. Alors, permutant certaines lignes et colonnes, nous sommes ramenés au cas où a_{11} n'est pas nul. Multipliant la première ligne par a_{11}^{-1}, l'élément a_{11} devient égal à l'unité. Retranchant de la $j^{\text{ème}}$ colonne la première colonne multipliée par a_{1j}, $j > 1$, l'élément a_{1j} est remplacé par l'élément nul. Transformant de cette manière toutes les colonnes à partir de la seconde, ainsi que toutes les lignes, nous sommes ramenés à une matrice de la forme

$$A' = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & a_{22}' & \ldots & a_{2n}' \\ \cdot & \cdot & \cdot \; \cdot & \cdot \\ 0 & a_{s2}' & \ldots & a_{sn}' \end{pmatrix}.$$

Opérant de la même façon sur la matrice à éléments a_{ij}' ayant $(s-1)$ lignes et $(n-1)$ colonnes et ainsi de suite, nous obtenons, après un nombre fini de pas, une matrice diagonale, ayant le même rang que la matrice initiale A.

Ainsi, *pour calculer le rang d'une matrice il faut la réduire d'abord à la forme diagonale; le nombre d'éléments de la diagonale principale qui sont égaux à l'unité est le rang de la matrice initiale.*

Exemple. Calculer le rang de la matrice

$$A=\begin{pmatrix} 0 & 2 & -4 \\ -1 & -4 & 5 \\ 3 & 1 & 7 \\ 0 & 5 & -10 \\ 2 & 3 & 0 \end{pmatrix}.$$

Permutant la première et la seconde colonne, puis multipliant la première ligne par $\frac{1}{2}$, il vient

$$\begin{pmatrix} 1 & 0 & -2 \\ -4 & -1 & 5 \\ 1 & 3 & 7 \\ 5 & 0 & -10 \\ 3 & 2 & 0 \end{pmatrix}.$$

Ajoutant à la troisième colonne la première multipliée par 2, puis ajoutant la nouvelle première ligne multipliée par des nombres convenablement choisis aux autres lignes de la matrice, il vient

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -3 \\ 0 & 3 & 9 \\ 0 & 0 & 0 \\ 0 & 2 & 6 \end{pmatrix}.$$

Enfin, multipliant la seconde ligne par -1, retranchant la seconde colonne, multipliée par 3, de la troisième, puis retranchant la nouvelle seconde ligne, multipliée par des entiers convenablement choisis, de la troisième et de la cinquième ligne, nous sommes ramenés à la forme diagonale cherchée

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Donc, le rang de la matrice A est deux.

Nous reviendrons encore dans le chapitre XIII aux transformations élémentaires et aux formes diagonales des matrices ; ces matrices auront cependant pour éléments non plus des nombres, mais des polynômes.

§ 11. Systèmes d'équations linéaires

A présent, nous sommes en mesure d'aborder l'étude des systèmes d'équations linéaires arbitraires, sans nous restreindre au cas où le nombre des inconnues est égal à celui des équations. Nos résultats serons toutefois valables dans le cas où le nombre des équations coïncide avec celui des inconnues, mais le déterminant du système est nul (ce cas n'ayant pas été étudié au § 7).

Soit un système d'équations linéaires

$$\left.\begin{array}{l} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=b_1, \\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{s1}x_1+a_{s2}x_2+\ldots+a_{sn}x_n=b_s. \end{array}\right\} \quad (1)$$

Comme on le sait du § 1, il faut d'abord vérifier si le système (1) est compatible. Pour cela formons la matrice A des coefficients du système et la matrice « élargie » $\bar{A}$ qui s'obtient de A en complétant ses colonnes de la colonne des seconds membres du système (1):

$$A=\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{s1} & a_{s2} & \ldots & a_{sn} \end{pmatrix}, \qquad \bar{A}=\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & b_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{s1} & a_{s2} & \ldots & a_{sn} & b_s \end{pmatrix}$$

et calculons leur rang. Il est facile de voir que le *rang de la matrice $\bar{A}$ est égal à celui de A, ou lui est supérieur d'une unité.* En effet, prenons un système maximal quelconque des colonnes de la matrice A. Ce système, considéré dans la matrice $\bar{A}$, sera également linéairement indépendant. S'il est maximal dans le système des colonnes de la matrice $\bar{A}$, alors la colonne des seconds membres est une combinaison linéaire des autres colonnes de $\bar{A}$, c'est-à-dire le rang de A est égal à celui de $\bar{A}$; dans le cas contraire, ajoutant au système maximal de la matrice A la colonne des seconds membres, nous obtenons un système maximal de la matrice $\bar{A}$.

Le problème de compatibilité des systèmes d'équations linéaires est entièrement résolu par le théorème suivant.

Théorème de Kronecker-Capelli. *Un système d'équations linéaires* (1) *est compatible si et seulement si le rang de sa matrice A est égal à celui de la matrice « élargie » $\bar{A}$.*

Démonstration. 1. Supposons le système (1) compatible et soit $k_1, k_2, \ldots, k_n$ l'une de ses solutions. Substituant dans (1) ces nombres à la place des inconnues, on obtient s identités montrant que la dernière colonne de la matrice $\bar{A}$ est une combinaison linéaire des autres colonnes de cette matrice, les coefficients de la combinaison linéaire étant respectivement $k_1, k_2, \ldots, k_n$. Toute colonne de $\bar{A}$, excepté la dernière, est aussi une colonne de la matrice A et ses éléments s'expriment donc linéairement par les éléments des autres colonnes de A. Il en résulte que les systèmes des colonnes des matrices A et $\bar{A}$ (considérées comme des vecteurs à s dimensions) sont équivalents et, par conséquent, ont le même rang, comme

on l'a déjà vu au § 9; autrement dit les matrices A et A ont le même rang.

2. A présent supposons que les matrices A et $\bar{A}$ aient le même rang. Il en découle que toute sous-famille maximale des colonnes de la matrice A l'est également dans le système des colonnes de la matrice $\bar{A}$. Ainsi, les éléments de la dernière colonne de $\bar{A}$ s'expriment linéairement par des éléments correspondants des colonnes du système maximal et, par conséquent, par des colonnes de la matrice A. Il existe donc une suite de coefficients telle que la combinaison linéaire des colonnes de A avec ces coefficients, soient k_1, k_2, . . ., k_n, donne la colonne des seconds membres du système (1). Cela signifie que les nombres k_1, k_2, . . ., k_n forment une solution de (1). Ainsi, l'identité des rangs des matrices A et $\bar{A}$ entraîne la compatibilité du système (1).

Le théorème est démontré. Son application à des exemples concrets nécessite, avant tout, le calcul du rang de la matrice A; pour cela il faut trouver un mineur non nul de A, soit M, tel que tous les mineurs contenant M soient nuls. Ensuite, il suffit de vérifier que tout mineur de la matrice $\bar{A}$, qui contient M et qui n'est pas un mineur de A, est également nul (on appelle ces mineurs *déterminants caractéristiques* du système (1)). S'il en est ainsi, les rangs de A et $\bar{A}$ coïncident et le système (1) est compatible; dans le cas contraire, c'est-à-dire si au moins un des déterminants caractéristiques est non nul, le système (1) est incompatible. Ainsi, on peut encore énoncer le théorème de Kronecker-Capelli comme suit: *un système d'équations linéaires* (1) *est compatible si et seulement si tous ses déterminants caractéristiques sont nuls.*

A présent, supposons que le *système* (1) *soit compatible*. Le théorème de Kronecker-Capelli permet d'établir la compatibilité de (1) et garantit l'existence d'une solution de ce système, mais ne donne pas le *moyen pratique de trouver toutes les solutions* d'un système donné. Nous allons nous occuper de ce problème.

Soit une matrice A de rang r. Selon le paragraphe précédent, le rang r est le nombre maximal de lignes linéairement indépendantes de la matrice A. Pour fixer les idées, supposons que les r premières lignes de A soient linéairement indépendantes et que toutes les autres lignes soient leurs combinaisons linéaires. Alors, les r premières lignes de la matrice $\bar{A}$ seront également linéairement indépendantes, car s'il en était autrement, cela signifierait que les r premières lignes de A sont linéairement dépendantes (voir l'addition des vecteurs). L'identité des rangs de A et de $\bar{A}$ entraîne que les r premières lignes de $\bar{A}$ forment une sous-famille maximale dans le système des lignes de la matrice $\bar{A}$. Autrement dit, toute

ligne de $\overline{A}$ est une combinaison linéaire des r premières lignes de cette matrice.

Il en résulte que toute équation du système (1) est une combinaison linéaire des r premières équations avec certains coefficients de sorte que toute solution des r premières équations satisfait également à toutes les équations du système (1). Il suffit, donc, de trouver toutes les solutions du système:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rn}x_n = b_r. \end{array}\right\} \quad (2)$$

Les lignes formées par les coefficients des inconnues dans les équations (2) étant linéairement indépendantes, c'est-à-dire la matrice des coefficients de (2) étant de rang r, il en résulte que $r \leqslant n$ et que, de plus, la matrice du système (2) possède au moins un mineur d'ordre r non nul. Si $r = n$, le système (2) a le même nombre d'équations et d'inconnues et son déterminant n'est pas nul; dans ce cas ce système, ainsi que le système (1), possède une solution, qu'on peut calculer par les formules de Cramer.

Soit, à présent, $r < n$. Pour fixer les idées, supposons que le mineur d'ordre r formé par les coefficients des r premières inconnues soit non nul. Faisons passer dans les seconds membres des équations (2) tous les termes contenant les inconnues $x_{r+1}, \ldots, x_n$ auxquelles nous attribuerons, respectivement, les valeurs $c_{r+1}, \ldots, c_n$. Nous obtenons un système de r équations à r inconnues $x_1, x_2, \ldots, x_r$:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1r}x_r = b_1 - a_{1,\,r+1}c_{r+1} - \ldots - a_{1n}c_n, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2r}x_r = b_2 - a_{2,\,r+1}c_{r+1} - \ldots - a_{2n}c_n, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + a_{r2}x_2 + \ldots + a_{rr}x_r = b_r - a_{r,\,r+1}c_{r+1} - \ldots - a_{rn}c_n. \end{array}\right\} \quad (3)$$

On peut appliquer à ce système les formules de Cramer de sorte qu'il possède une solution unique $c_1, c_2, \ldots, c_r$; il est clair que les nombres $c_1, \ldots, c_r, c_{r+1}, \ldots, c_n$ forment une solution du système (2). Comme les valeurs $c_{r+1}, \ldots, c_n$ des inconnues $x_{r+1}, \ldots, x_n$, dites *non principales*, étaient choisies arbitrairement, nous obtenons de cette manière une infinité de solutions distinctes du système (2).

D'autre part, toute solution de (2) peut être obtenue par ce procédé. En effet, soit $c_1, c_2, \ldots, c_n$ une solution quelconque de (2); prenons pour valeurs des inconnues non principales les nombres $c_{r+1}, \ldots, c_n$. Alors, les nombres $c_1, c_2, \ldots, c_r$ vérifient le système (3) et, par conséquent, ils forment la solution unique de (3) qui est représentée par les formules de Cramer.

Tout ce qu'on vient de dire peut être résumé de façon suivante en une *règle de résolution des systèmes arbitraires d'équations linéaires*:

Soit un système compatible d'équations linéaires (1) *dont la matrice des coefficients A est de rang r. Fixons r lignes linéairement indépendantes quelconques de A et conservons les équations de* (1) *qui correspondent aux lignes fixées. Dans ces équations choisissons r inconnues de telle manière que le déterminant d'ordre r formé par leurs coefficients soit non nul et faisons passer les autres inconnues dans les seconds membres des équations correspondantes. Attribuant aux inconnues non principales des valeurs arbitraires et calculant au moyen des formules de Cramer les valeurs des inconnues principales, nous obtenons toutes les solutions du système* (1).

Résumons encore une fois le résultat obtenu ci-dessus:

Pour qu'un système compatible (1) *ait une solution unique, il faut et il suffit que le rang de la matrice du système soit égal au nombre des inconnues.*

Exemples. 1. Résoudre le système:

$$\left.\begin{aligned} 5x_1 - x_2 + 2x_3 + x_4 &= 7, \\ 2x_1 + x_2 + 4x_3 - 2x_4 &= 1, \\ x_1 - 3x_2 - 6x_3 + 5x_4 &= 0. \end{aligned}\right\}$$

Le rang de la matrice des coefficients est deux, car le mineur d'ordre deux formé par les deux premières lignes et les deux premières colonnes est non nul et les deux mineurs d'ordre trois qui le contiennent sont nuls. Le rang de la matrice « élargie » est trois, car

$$\begin{vmatrix} 5 & -1 & 7 \\ 2 & 1 & 1 \\ 1 & -3 & 0 \end{vmatrix} = -35 \neq 0.$$

Le système est donc incompatible.

2. Résoudre le système:

$$\left.\begin{aligned} 7x_1 + 3x_2 &= 2, \\ x_1 - 2x_2 &= -3, \\ 4x_1 + 9x_2 &= 11. \end{aligned}\right\}$$

La matrice des coefficients est de rang deux, c'est-à-dire son rang coïncide avec le nombre des inconnues; la matrice « élargie » est aussi de rang deux. Le système est donc compatible et possède une solution unique; les premiers membres des deux premières équations sont linéairement indépendants; résolvant le système de ces deux équations, nous trouvons les valeurs des inconnues:

$$x_1 = -\frac{5}{17}, \quad x_2 = \frac{23}{17}.$$

Il est facile de vérifier que ces valeurs satisfont à la troisième équation du système initial.

3. Résoudre le système:

$$\left.\begin{aligned} x_1 + x_2 - 2x_3 - x_4 + x_5 &= 1, \\ 3x_1 - x_2 + x_3 + 4x_4 + 3x_5 &= 4, \\ x_1 + 5x_2 - 9x_3 - 8x_4 + x_5 &= 0. \end{aligned}\right\}$$

Le système est compatible, car la matrice « élargie » est de même rang que la matrice des coefficients, ce dernier étant égal à deux. Les premiers membres de la première et de la troisième équation sont linéairement indépendants, car les coefficients de x_1 et de x_2 dans ces équations forment un mineur d'ordre deux non nul. Résolvons le système formé par la première et la troisième équation du système initial (ici les inconnues x_3, x_4, x_5 sont non principales et on les fait passer dans les seconds membres des équations correspondantes, en leur attribuant les valeurs numériques). Appliquant les formules de Cramer, on trouve les valeurs des inconnues principales x_1 et x_2:

$$x_1=\frac{5}{4}+\frac{1}{4}x_3-\frac{3}{4}x_4-x_5,$$

$$x_2=-\frac{1}{4}+\frac{7}{4}x_3+\frac{7}{4}x_4.$$

Ces égalités donnent la *solution générale* du système considéré: les inconnues non principales prenant des valeurs numériques arbitraires, nous obtenons toutes les solutions de notre système. Ainsi, les vecteurs (2, 5, 3, 0, 0), (3, 5, 2, 1, —2), $\left(0, -\frac{1}{4}, -1, 1, \frac{1}{4}\right)$, etc., sont des solutions du système en question. D'autre part, substituant dans chaque équation du système donné aux inconnues x_1 et x_2 leurs expressions obtenues ci-dessus en fonction de x_3, x_4, x_5, l'équation est identiquement vérifiée; par exemple, on vérifie aisément qu'en substituant dans la seconde équation à x_1 et x_2 leurs expressions on obtient une identité.

4. Résoudre le système:

$$\left.\begin{aligned}4x_1+x_2-2x_3+x_4&=3,\\x_1-2x_2-x_3+2x_4&=2,\\2x_1+5x_2\qquad-x_4&=-1,\\3x_1+3x_2-x_3-3x_4&=1.\end{aligned}\right\}$$

Bien que le nombre des inconnues soit égal à celui des équations, on ne peut pas appliquer les formules de Cramer, le déterminant du système étant nul. La matrice des coefficients est de rang trois, son mineur d'ordre trois à l'angle droit en haut étant non nul. La matrice « élargie » étant également de rang trois, le système donné est compatible. Ne considérant que les trois premières équations et l'inconnue x_1 étant non principale, on trouve aisément la solution générale:

$$x_2=-\frac{1}{5}-\frac{2}{5}x_1,\quad x_3=-\frac{8}{5}+\frac{9}{5}x_1,\quad x_4=0.$$

5. Soit un système de $(n+1)$ équations à n inconnues. La matrice « élargie » $\overline{A}$ de ce système est une matrice carrée d'ordre $(n+1)$. Si notre système est compatible, alors en vertu du théorème de Kronecker-Capelli, le déterminant de la matrice $\overline{A}$ est nul.

Ainsi, soit donné le système

$$\left.\begin{aligned}x_1-8x_2&=\\2x_1+x_2&=1,\\4x_1+7x_2&=-4.\end{aligned}\right\}$$

Le déterminant, formé par les coefficients et les seconds membres, est non nul :

$$\begin{vmatrix} 1 & -8 & 3 \\ 2 & 1 & 1 \\ 4 & 7 & -4 \end{vmatrix} = -77,$$

le système est donc incompatible.

La réciproque n'est pas vraie en général: si le déterminant de la matrice $\bar{A}$ est nul, cela n'entraîne pas nécessairement que le rang de A soit égal à celui de $\bar{A}$.

§ 12. Systèmes d'équations linéaires homogènes

Appliquons les résultats du paragraphe précédent à un *système d'équations linéaires homogènes*:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{s1}x_1 + a_{s2}x_2 + \ldots + a_{sn}x_n = 0. \end{array}\right\} \quad (1)$$

Un système homogène, selon le théorème de Kronecker-Capelli, est toujours compatible. En effet, si on ajoute à un système des colonnes la colonne identiquement nulle, le rang en reste invariant. D'ailleurs, comme le système (1) a pour solution le vecteur nul (0, 0, . . ., 0), la compatibilité de (1) est évidente.

Supposons que la matrice A des coefficients du système (1) soit de rang r. *Si $r = n$, alors la solution nulle est la solution unique du système* (1); *pour $r < n$, le système* (1) *possède d'autres solutions, non nulles*, et pour les trouver toutes on utilise le même procédé que dans le cas d'un système arbitraire. Notamment, *un système de n équations linéaires homogènes à n inconnues possède des solutions non nulles si et seulement si son déterminant est nul* [1]. En effet, si le déterminant du système est nul, cela signifie que le rang de la matrice A est strictement inférieur à n. D'autre part, *si dans un système d'équations linéaires homogènes le nombre des équations est inférieur à celui des inconnues, le système possède des solutions non nulles*, car, dans ce cas, le rang de la matrice ne peut pas être égal au nombre des inconnues; ce résultat avait déjà été obtenu au § 1 par d'autres raisonnements.

Considérons, en particulier, un système de $(n - 1)$ équations linéaires homogènes à n inconnues et supposons que les *premiers membres de ces équa-*

---

[1] La nécessité de cette condition a été montrée au § 7.

tions soient linéairement indépendants. Soit

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n-1,1} & a_{n-1,2} & \dots & a_{n-1,n} \end{pmatrix}$$

la matrice des coefficients de ce système; soit M_i le mineur d'ordre $(n-1)$ que l'on obtient de la matrice A en supprimant sa $i^{\text{ème}}$ colonne, $i=1, 2, \dots, n$. *Alors une des solutions de notre système est de la forme*

$$M_1, \ -M_2, \ M_3, \ -M_4, \ \dots, \ (-1)^{n-1} M_n, \tag{2}$$

et toute autre solution est proportionnelle à celle-ci.

Démonstration. Par hypothèse, le rang de la matrice A étant $n-1$, un des mineurs M_i, soit M_n, est différent de zéro. Prenons x_n pour inconnue non principale et faisons passer les termes contenant x_n dans les seconds membres des équations correspondantes; il vient

$$\begin{gathered} a_{11}x_1+a_{12}x_2+\dots+a_{1,n-1}x_{n-1}=-a_{1n}x_n, \\ a_{21}x_1+a_{22}x_2+\dots+a_{2,n-1}x_{n-1}=-a_{2n}x_n, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n-1,1}x_1+a_{n-1,2}x_2+\dots+a_{n-1,n-1}x_{n-1}=-a_{n-1,n}x_n. \end{gathered}$$

Appliquant ensuite les formules de Cramer, on trouve la solution générale du système donné, qui, après quelques transformations évidentes, prend la forme

$$x_i=(-1)^{n-i}\frac{M_i}{M_n}x_n, \qquad i=1, 2, \dots, n-1. \tag{3}$$

Posant $x_n=(-1)^{n-1}M_n$, on trouve: $x_i=(-1)^{2n-i-1}M_i$, $i=1, 2, \dots, n-1$, ou encore $x_i=(-1)^{i-1}M_i$, la différence $(2n-i-1)-(i-1)=2n-2i$ étant paire; autrement dit, les nombres (2) donnent réellement une solution de notre système. Toute autre solution du système s'obtient des formules (3) en attribuant à l'inconnue x_n une autre valeur numérique et, par conséquent, cette solution est proportionnelle à la solution (2). Evidemment, notre proposition est encore valable si $M_n=0$, mais un des mineurs M_i, $1 \leqslant i \leqslant n-1$, est non nul.

Les solutions des systèmes d'équations linéaires homogènes jouissent des propriétés suivantes. Le vecteur $\beta=(b_1, b_2, \dots, b_n)$ étant solution du système (1), le vecteur $k\beta=(kb_1, kb_2, \dots, kb_n)$, où k est un nombre quelconque, l'est aussi. On vérifie cela directement en substituant les composantes du vecteur $k\beta$ aux inconnues $x_1, \dots, x_n$ dans les équations (1). Puis, le vecteur $\gamma=(c_1, c_2, \dots, c_n)$ étant une autre solution du système (1), le vecteur $\beta+\gamma=(b_1+c_1, b_2+c_2, \dots, b_n+c_n)$ l'est également; en effet,

$$\sum_{j=1}^{n} a_{ij}(b_j+c_j)=\sum_{j=1}^{n} a_{ij}b_j+\sum_{j=1}^{n} a_{ij}c_j=0, \qquad i=1, 2, \dots, s.$$

Plus généralement, *toute combinaison linéaire des solutions d'un système homogène* (1) *est encore une solution de ce système.* Notons que pour un système *non homogène*, dont les seconds membres ne sont pas tous nuls, la proposition correspondante n'est pas vraie:

la somme de deux solutions, ni le produit d'une solution par un scalaire n'est plus solution du système non homogène.

Comme on le sait du § 9, tout ensemble de vecteurs à n dimensions, contenant plus de n vecteurs, constitue une famille non libre. Il en résulte que l'on peut choisir dans l'ensemble de solutions d'un système homogène, qui sont des vecteurs à n dimensions, une sous-famille maximale *finie* de sorte que toute solution de (1) soit une combinaison linéaire des vecteurs linéairement indépendants de cette sous-famille. On appelle *famille fondamentale de solutions* d'un système homogène (1) toute famille maximale appartenant à l'ensemble des solutions de (1).

Notons une fois de plus qu'un *vecteur à n dimensions est solution du système* (1) *si et seulement si ce vecteur est une combinaison linéaire des vecteurs d'une famille fondamentale de solutions de* (1).

Il est clair qu'une famille fondamentale de solutions n'existe que lorsque le système (1) possède des solutions non nulles, c'est-à-dire si le rang de la matrice des coefficients de (1) est inférieur au nombre d'inconnues. S'il en est ainsi, le système peut posséder plusieurs familles fondamentales distinctes. Toutes les familles fondamentales sont, néanmoins, équivalentes, car chaque vecteur d'une famille fondamentale s'exprime linéairement par les vecteurs d'une autre famille fondamentale, de sorte que toutes les familles fondamentales *ont un même nombre de vecteurs solutions.*

Le théorème suivant est valable:

Soient r le rang de la matrice des coefficients du système (1), *n le nombre d'inconnues, et supposons que* $r < n$. *Toute famille fondamentale de solutions contient exactement* $(n - r)$ *vecteurs solutions de* (1).

Pour démontrer ce théorème, notons que le nombre des inconnues non principales est exactement $(n - r)$; supposons que les inconnues $x_{r+1}, x_{r+2}, \ldots, x_n$ soient non principales. Soit d un déterminant d'ordre $(n - r)$ quelconque, $d \neq 0$, que nous écrivons sous la forme:

$$d = \begin{vmatrix} c_{1,r+1}, & c_{1,r+2}, & \ldots, & c_{1n} \\ c_{2,r+1}, & c_{2,r+2}, & \ldots, & c_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ c_{n-r,r+1}, & c_{n-r,r+2}, & \ldots, & c_{n-r,n} \end{vmatrix}.$$

Prenant les éléments de la $i^{\text{ème}}$ ligne pour valeurs des inconnues non principales, nous obtenons, comme on le sait déjà, des valeurs bien déterminées pour les inconnues $x_1, x_2, \ldots, x_r$, soit respectivement $c_{i1}, c_{i2}, \ldots, c_{ir}$, c'est-à-dire une solution bien déterminée du système (1):

$$\alpha_i = (c_{i1}, c_{i2}, \ldots, c_{ir}, c_{i,r+1}, c_{i,r+2}, \ldots, c_{in}),$$

pour tout i, $i = 1, 2, \ldots, n - r$.

L'ensemble de vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_{n-r}$, obtenu par ce procédé, est une famille fondamentale de solutions du système (1). En effet, les vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_{n-r}$ sont linéairement indépendants, car la matrice, dont les lignes sont ces vecteurs, a un mineur d'ordre $(n-r)$ non nul, à savoir le mineur d. D'autre part, soit

$$\beta = (b_1, b_2, \ldots, b_r, b_{r+1}, b_{r+2}, \ldots, b_n)$$

une solution quelconque du système d'équations (1). Montrons que β est une combinaison linéaire des vecteurs $\alpha_1, \alpha_2, \ldots, \alpha_{n-r}$.

Notons par α'_i, $i = 1, 2, \ldots, n-r$, la $i^{\text{ème}}$ ligne du déterminant d considérée comme un vecteur à $(n-r)$ dimensions. Posons, ensuite

$$\beta' = (b_{r+1}, b_{r+2}, \ldots, b_n).$$

Les vecteurs α'_i, $i = 1, 2, \ldots, n-r$, sont linéairement indépendants, car $d \neq 0$. Or, l'ensemble de vecteurs à $(n-r)$ dimensions

$$\alpha'_1, \alpha'_2, \ldots, \alpha'_{n-r}, \beta'$$

est linéairement dépendant, car le nombre de ses vecteurs est plus grand que celui des composantes de chaque vecteur. Il existe, donc, des nombres $k_1, k_2, \ldots, k_{n-r}$ tels que

$$\beta' = k_1\alpha'_1 + k_2\alpha'_2 + \ldots + k_{n-r}\alpha'_{n-r}. \tag{4}$$

Considérons à présent le vecteur à n dimensions

$$\delta = k_1\alpha_1 + k_2\alpha_2 + \ldots + k_{n-r}\alpha_{n-r} - \beta.$$

Le vecteur δ étant une combinaison linéaire des vecteurs solutions du système homogène (1), il est, à son tour, une solution de (1). Comme il vient de (4), les inconnues non principales de la solution δ sont nulles. Or, l'unique solution du système (1) qui corresponde aux valeurs nulles des inconnues non principales est la solution nulle. Ainsi, $\delta = 0$, c'est-à-dire

$$\beta = k_1\alpha_1 + k_2\alpha_2 + \ldots + k_{n-r}\alpha_{n-r}.$$

Le théorème est démontré.

Notons que la démonstration qui vient d'être donnée permet d'affirmer que *toute* famille fondamentale de solutions d'un système homogène (1) peut être obtenue en choisissant convenablement le déterminant d d'ordre $(n-r)$.

Exemple. Soit le système d'équations linéaires homogènes

$$\left.\begin{aligned} 3x_1 + x_2 - 8x_3 + 2x_4 + x_5 &= 0, \\ 2x_1 - 2x_2 - 3x_3 - 7x_4 + 2x_5 &= 0, \\ x_1 + 11x_2 - 12x_3 + 34x_4 - 5x_5 &= 0, \\ x_1 - 5x_2 + 2x_3 - 16x_4 + 3x_5 &= 0. \end{aligned}\right\}$$

Le rang de la matrice de ses coefficients est deux, le nombre d'inconnues est cinq ; donc, toute famille fondamentale de solutions de ce système est composée de trois vecteurs solutions. Résolvons ce système en prenant pour inconnues non principales x_3, x_4, x_5 et en nous bornant aux deux premières équations. Nous obtenons la solution générale sous la forme

$$x_1=\frac{19}{8}x_3+\frac{3}{8}x_4-\frac{1}{2}x_5,$$

$$x_2=\frac{7}{8}x_3-\frac{25}{8}x_4+\frac{1}{2}x_5.$$

Considérons les trois vecteurs linéairement indépendants à trois dimensions: (1, 0, 0), (0, 1, 0), (0, 0, 1). Substituant les composantes de chaque vecteur aux inconnues non principales dans les formules de la solution générale et calculant les valeurs correspondantes des inconnues x_1 et x_2, nous trouvons une famille fondamentale de solutions du système d'équations donné:

$$\alpha_1=\left(\frac{19}{8},\ \frac{7}{8},\ 1,\ 0,\ 0\right),\qquad \alpha_2=\left(\frac{3}{8},\ -\frac{25}{8},\ 0,\ 1,\ 0\right),$$

$$\alpha_3=\left(-\frac{1}{2},\ \frac{1}{2},\ 0,\ 0,\ 1\right).$$

Terminons ce paragraphe en établissant la relation qui existe entre les solutions des systèmes homogènes et des systèmes non homogènes.

Soit un système d'équations linéaires non homogènes:

$$\left.\begin{array}{l} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=b_1,\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=b_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ a_{s1}x_1+a_{s2}x_2+\ldots+a_{sn}x_n=b_s. \end{array}\right\}\qquad(5)$$

Le système d'équations linéaires homogènes:

$$\left.\begin{array}{l} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=0,\\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ a_{s1}x_1+a_{s2}x_2+\ldots+a_{sn}x_n=0, \end{array}\right\}\qquad(6)$$

obtenu du système (5) en remplaçant tous les b_i par 0, est dit *système* homogène *associé* au système (5). Il y a une relation intime entre les solutions des systèmes (5) et (6), comme le montrent les deux théorèmes suivants.

I. *La somme d'une solution quelconque du système* (5) *et d'une solution quelconque du système* (6) *est encore une solution de* (5).

En effet, soient $c_1, c_2, \ldots, c_n$ et $d_1, d_2, \ldots, d_n$ deux solutions quelconques respectivement de (5) et de (6). Considérons une équation quelconque de (5), soit la $k^{\text{ème}}$, et remplaçons dans cette équation les inconnues par les nombres c_1+d_1, c_2+d_2, $\ldots$, c_n+d_n.

Il vient :

$$\sum_{j=1}^{n} a_{kj}(c_j+d_j)=\sum_{j=1}^{n} a_{kj}c_j+\sum_{j=1}^{n} a_{kj}d_j=b_k+0=b_k.$$

II. *La différence de deux solutions quelconques du système* (5) *est une solution du système* (6).

En effet, soient $c_1, c_2, \ldots, c_n$ et $c'_1, c'_2, \ldots, c'_n$ deux solutions quelconques de (5). Alors, remplaçant les inconnues $x_1, \ldots, x_n$, dans les équations (6), par les nombres

$$c_1-c'_1,\ c_2-c'_2,\ \ldots,\ c_n-c'_n,$$

il vient :

$$\sum_{j=1}^{n} a_{kj}(c_j-c'_j)=\sum_{j=1}^{n} a_{kj}c_j-\sum_{j=1}^{n} a_{kj}c'_j=b_k-b_k=0,$$

pour tout k, $k=1, 2, \ldots, s$.

Il résulte de ces théorèmes que *pour trouver la solution générale du système non homogène* (5), *il faut d'abord en trouver une solution particulière, puis l'ajouter à la solution générale du système homogène* (6) *associé au système* (5).

Chapitre III

ALGÈBRE DES MATRICES

§ 13. Multiplication des matrices

La notion de matrice introduite dans les chapitres précédents a été utilisée comme un outil auxiliaire, mais essentiel, pour l'étude des systèmes d'équations linéaires. Les nombreuses autres applications de cette notion en ont fait l'objet d'une grande théorie autonome qui en maintes parties sort du cadre de notre cours. Nous nous occuperons des fondements de cette théorie en commençant par introduire deux opérations algébriques dans l'ensemble des matrices carrées d'un même ordre : l'addition et la multiplication. Nous allons commencer par la multiplication ; l'addition sera définie au § 15.

On connaît du cours de géométrie analytique les formules de passage d'un système orthogonal de coordonnées à un autre système orthogonal qui correspondent à une rotation du plan autour de l'origine :

$$x = x' \cos\alpha - y' \sin\alpha,$$
$$y = x' \sin\alpha + y' \cos\alpha.$$

Ici α est l'angle de rotation, x, y et x', y' sont respectivement les anciennes et les nouvelles coordonnées d'un point du plan ; ainsi, x et y s'expriment linéairement par x' et y' avec certains coefficients numériques. Il y a d'autres cas où il est nécessaire d'avoir recours aux changements d'indéterminées (ou de variables), dans lesquels les anciennes indéterminées sont des fonctions linéaires des nouvelles ; on a l'habitude d'appeler un tel changement d'indéterminées transformation linéaire (ou substitution linéaire). Nous sommes donc conduits à la définition suivante :

On appelle *transformation linéaire d'indéterminées* tout passage d'un système de n indéterminées $x_1, x_2, \ldots, x_n$ à un système de n indéterminées $y_1, y_2, \ldots, y_n$ tel que les indéterminées $x_1, x_2, \ldots, x_n$ sont des fonctions linéaires des nouvelles indéterminées $y_1, y_2, \ldots, y_n$ avec certains coefficients numériques, à savoir :

$$\left.\begin{aligned} x_1 &= a_{11}y_1 + a_{12}y_2 + \ldots + a_{1n}y_n, \\ x_2 &= a_{21}y_1 + a_{22}y_2 + \ldots + a_{2n}y_n, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ x_n &= a_{n1}y_1 + a_{n2}y_2 + \ldots + a_{nn}y_n. \end{aligned}\right\} \quad (1)$$

La transformation linéaire (1) est bien définie par la matrice de ses coefficients

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix},$$

car si deux transformations linéaires ont une même matrice, elles coïncident à cette différence près que les indéterminées peuvent être notées différemment; évidemment on peut convenir que le choix de notations dépend uniquement de nous. Inversement, en partant d'une matrice carrée d'ordre n on trouve immédiatement les formules de la transformation linéaire correspondante pour laquelle cette matrice est la matrice des coefficients. Ainsi, il existe une correspondance bijective entre les transformations linéaires de n indéterminées et les matrices carrées d'ordre n, de sorte que toute notion (ou toute propriété) concernant les transformations linéaires correspond à la notion (ou à la propriété) analogue se rapportant aux matrices et inversement.

Considérons le résultat de l'application successive de deux transformations linéaires. Après la transformation linéaire (1) appliquons la transformation

$$\left.\begin{aligned} y_1 &= b_{11}z_1 + b_{12}z_2 + \dots + b_{1n}z_n, \\ y_2 &= b_{21}z_1 + b_{22}z_2 + \dots + b_{2n}z_n, \\ &\dots\dots\dots\dots\dots\dots \\ y_n &= b_{n1}z_1 + b_{n2}z_2 + \dots + b_{nn}z_n, \end{aligned}\right\} \tag{2}$$

qui fait correspondre au système des indéterminées $y_1, y_2, \dots, y_n$ le système des indéterminées $z_1, z_2, \dots, z_n$; soit B la matrice de cette transformation. Remplaçant dans (1) les indéterminées $y_1, y_2, \dots, y_n$ d'après les formules (2) nous sommes conduits aux expressions linéaires des indéterminées $x_1, x_2, \dots, x_n$ par les indéterminées $z_1, z_2, \dots, z_n$. Ainsi, le *résultat de l'application successive de deux transformations linéaires des indéterminées est encore une transformation linéaire*.

Exemple. L'application de deux transformations linéaires

$$\begin{aligned} x_1 &= 3y_1 - y_2, & y_1 &= z_1 + z_2, \\ x_2 &= y_1 + 5y_2, & y_2 &= 4z_1 + 2z_2 \end{aligned}$$

est la transformation linéaire

$$\begin{aligned} x_1 &= 3(z_1 + z_2) - (4z_1 + 2z_2) = -z_1 + z_2, \\ x_2 &= (z_1 + z_2) + 5(4z_1 + 2z_2) = 21z_1 + 11z_2. \end{aligned}$$

Soit C la matrice des coefficients de la transformation linéaire qui est le résultat de l'application successive des transformations (1) et (2); nous allons trouver les expressions des éléments c_{ik}, $i, k = 1, 2, \ldots, n$, de cette matrice par les éléments des matrices A et B. Utilisant le signe Σ pour récrire les transformations (1) et (2) sous la forme

$$x_i = \sum_{j=1}^{n} a_{ij}, \ y_j, \quad i = 1, 2, \ldots, n; \quad y_j = \sum_{k=1}^{n} b_{jk} z_k, \qquad j = 1, 2, \ldots, n,$$

il vient

$$x_i = \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{n} b_{jk} z_k \right) = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) z_k, \qquad i = 1, 2, \ldots, n.$$

Ainsi, le coefficient de z_k dans l'expression de x_i, c'est-à-dire l'élément c_{ik} de la matrice C, est de la forme

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} = a_{i1} b_{1k} + a_{i2} b_{2k} + \ldots + a_{in} b_{nk}\,; \tag{3}$$

l'élément de la matrice C qui se trouve à l'intersection de la $i^{\text{ème}}$ ligne et de la $k^{\text{ème}}$ colonne est égal à la somme des produits des éléments de la $i^{\text{ème}}$ ligne de la matrice A par les éléments de la $k^{\text{ème}}$ colonne de la matrice B.

La formule (3) donnant l'expression des éléments de la matrice C en fonction des éléments des matrices A et B permet de trouver directement la matrice C, sans qu'il soit nécessaire de considérer les transformations linéaires de matrices A et B. De cette manière on fait correspondre à tout couple de matrices carrées d'ordre n une troisième matrice bien déterminée du même ordre. Autrement dit, nous avons défini sur l'ensemble des matrices carrées d'ordre n une opération algébrique; cette opération est appelée *multiplication des matrices*, la matrice C est le *produit* de la matrice A par la matrice B:

$$C = AB.$$

Enonçons, une fois de plus, la relation qui existe entre les transformations linéaires et la multiplication des matrices:

La transformation linéaire des indéterminées qui s'obtient à la suite de l'application successive de deux transformations linéaires, dont les matrices des coefficients sont respectivement A et B, a pour matrice des coefficients la matrice AB.

Exemples.

1) $\begin{pmatrix} 4 & 9 \\ -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 4\cdot1+9\cdot(-2) & 4\cdot(-3)+9\cdot1 \\ (-1)\cdot1+3\cdot(-2) & (-1)\cdot(-3)+3\cdot1 \end{pmatrix} =$

$= \begin{pmatrix} -14 & -3 \\ -7 & 6 \end{pmatrix}.$

2) $\begin{pmatrix} 2 & 0 & 1 \\ -2 & 3 & 2 \\ 4 & -1 & 5 \end{pmatrix} \cdot \begin{pmatrix} -3 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & -1 & 3 \end{pmatrix} = \begin{pmatrix} -6 & 1 & 3 \\ 6 & 2 & 9 \\ -12 & -3 & 14 \end{pmatrix}.$

3) $\begin{pmatrix} 7 & 2 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 7 & 2 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 51 & 16 \\ 8 & 3 \end{pmatrix}.$

4) Trouver le résultat de l'application successive des deux transformations linéaires

$$\begin{aligned} x_1 &= 5y_1 - y_2 + 3y_3, \\ x_2 &= y_1 - 2y_2, \\ x_3 &= \quad 7y_2 - y_3 \end{aligned}$$

et

$$\begin{aligned} y_1 &= 2z_1 \quad + z_3, \\ y_2 &= \quad z_2 - 5z_3, \\ y_3 &= \quad 2z_2. \end{aligned}$$

Multipliant les matrices, il vient :

$$\begin{pmatrix} 5 & -1 & 3 \\ 1 & -2 & 0 \\ 0 & 7 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & -5 \\ 0 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 10 & 5 & 10 \\ 2 & -2 & 11 \\ 0 & 5 & -35 \end{pmatrix},$$

de sorte que la transformation linéaire en question est de la forme :

$$\begin{aligned} x_1 &= 10z_1 + 5z_2 + 10z_3, \\ x_2 &= 2z_1 - 2z_2 + 11z_3, \\ x_3 &= \quad 5z_2 - 35z_3. \end{aligned}$$

Revenons à un des exemples de multiplication des matrices, par exemple 2), et trouvons le produit de ces mêmes matrices en intervertissant l'ordre des facteurs. Il vient :

$$\begin{pmatrix} -3 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 1 \\ -2 & 3 & 2 \\ 4 & -1 & 5 \end{pmatrix} = \begin{pmatrix} -8 & 3 & -1 \\ 0 & 5 & 9 \\ 14 & -6 & 13 \end{pmatrix}.$$

Ainsi, la multiplication des matrices dépend essentiellement de l'ordre des facteurs, autrement dit, la *multiplication des matrices n'est pas commutative*. Il fallait, d'ailleurs, s'y attendre car dans la définition de la matrice C donnée par la formule (3) les matrices A et B n'interviennent pas de façon équivalente. En effet, cette formule utilise les lignes de A et les colonnes de B.

On peut donner pour tout n, à partir de $n = 2$, des exemples de couples de matrices d'ordre n qui ne commutent pas, c'est-à-dire le produit de telles matrices dépend essentiellement de l'ordre des facteurs (en particulier, les matrices d'ordre deux dans l'exemple 1) ne commutent pas). D'autre part, il peut arriver que deux matrices données sont commutatives, comme le montre l'exemple suivant:

$$\begin{pmatrix} 7 & -12 \\ -4 & 7 \end{pmatrix} \cdot \begin{pmatrix} 26 & 45 \\ 15 & 26 \end{pmatrix} = \begin{pmatrix} 26 & 45 \\ 15 & 26 \end{pmatrix} \cdot \begin{pmatrix} 7 & -12 \\ -4 & 7 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}.$$

La multiplication des matrices est associative; par conséquent, on peut parler du produit bien défini d'un nombre fini de matrices d'ordre n, l'ordre des facteurs devant être bien déterminé en raison de la non-commutativité de la multiplication.

Démonstration. Soient A, B et C trois matrices d'ordre n. Ecrivons ces matrices en indiquant leurs éléments génériques: $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$. Introduisons ensuite les notations:

$$AB = U = (u_{ij}), \qquad BC = V = (v_{ij}),$$
$$(AB)\,C = S = (s_{ij}), \qquad A\,(BC) = T = (t_{ij}).$$

Il faut démontrer l'égalité $(AB)\,C = A\,(BC)$ ou encore $S = T$. Or,

$$u_{il} = \sum_{k=1}^{n} a_{ik} b_{kl}, \qquad v_{kj} = \sum_{l=1}^{n} b_{kl} c_{lj},$$

et, en vertu des égalités $S = UC$, $T = AV$, il vient

$$s_{ij} = \sum_{l=1}^{n} u_{il} c_{lj} = \sum_{l=1}^{n} \sum_{k=1}^{n} a_{ik} b_{kl} c_{lj},$$
$$t_{ij} = \sum_{k=1}^{n} a_{ik} v_{kj} = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} b_{kl} c_{lj},$$

c'est-à-dire $s_{ij} = t_{ij}$ pour $i, j = 1, 2, \ldots, n$.

L'étude des autres propriétés de la multiplication des matrices fait appel à leurs déterminants. Pour simplifier l'écriture, nous conviendrons de noter le déterminant de la matrice A par $|A|$. Si le lecteur veut bien se donner la peine de calculer, dans les exemples précédents, les déterminants des matrices intervenant dans les produits correspondants et de comparer le produit de ces déterminants avec le déterminant du produit des matrices données, alors il verra une chose assez curieuse qui est exprimée par le *théorème* suivant *de la multiplication des déterminants*:

Le déterminant du produit d'un nombre fini de matrices d'ordre n est égal au produit des déterminants de ces matrices.

Il suffit de démontrer ce théorème dans le cas de deux matrices. Soient $A = (a_{ij})$ et $B = (b_{ij})$ deux matrices d'ordre n et soit $AB = C = (c_{ij})$. Formons le déterminant auxiliaire Δ d'ordre $2n$ de la manière suivante: la matrice A se trouve à l'intersection des n premières lignes et colonnes de Δ, la matrice B à l'intersection des n dernières lignes et colonnes; tous les autres éléments de Δ sont nuls, excepté ceux de la diagonale principale de la matrice se trouvant à l'intersection des n dernières lignes et des n premières colonnes qui sont tous égaux à -1. Ainsi, le déterminant Δ est de la forme:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 0 \\ -1 & 0 & \dots & 0 & b_{11} & b_{12} & \dots & b_{1n} \\ 0 & -1 & \dots & 0 & b_{21} & b_{22} & \dots & b_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & -1 & b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix}.$$

D'après le théorème de Laplace, le développement du déterminant Δ par rapport aux mineurs extraits des n premières lignes nous donne l'égalité suivante:

$$\Delta = |A| \cdot |B|. \tag{4}$$

D'autre part, essayons de transformer le déterminant Δ, sans modifier sa valeur, de manière que les éléments b_{ij}, $i, j = 1, 2, \dots, n$, soient remplacés par des zéros. Pour cela, ajoutons à la $(n+1)^{\text{ème}}$ colonne de Δ sa première colonne multipliée par b_{11}, puis la deuxième colonne multipliée par b_{21} et ainsi de suite jusqu'à la $n^{\text{ème}}$ colonne multipliée par b_{n1}. Après quoi, ajoutons à la $(n+2)^{\text{ème}}$ colonne du déterminant Δ sa première colonne multipliée par b_{12}, la deuxième multipliée par b_{22}, etc. D'une façon générale, ajoutons à la $(n+j)^{\text{ème}}$ colonne de Δ la somme des n premières colonnes multipliées respectivement par les coefficients $b_{1j}, b_{2j}, \dots, b_{nj}$ et cela pour tous les j, $j = 1, 2, \dots, n$. Il est facile de vérifier que ces transformations nous conduisent à un autre déterminant dont la valeur est la même que celle du déterminant initial; en outre, dans le déterminant obtenu les éléments b_{ij} sont remplacés par des zéros. En même temps, à la place des éléments nuls qui se trouvaient à l'intersection des n premières lignes et des n dernières colonnes du déterminant donné on a les nombres suivants: à l'intersection de la $i^{\text{ème}}$ ligne et de la $(n+j)^{\text{ème}}$ colonne se trouve la somme $a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$ qui en vertu de (3) n'est autre que l'élément c_{ij} de la matrice $C = AB$ et cela pour tous les i et j,

$i, j = 1, 2, \ldots, n$. C'est donc la matrice C qui se trouve à présent à l'intersection des n premières lignes et des n dernières colonnes:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} & c_{11} & c_{12} & \ldots & c_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} & c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} & c_{n1} & c_{n2} & \ldots & c_{nn} \\ -1 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & -1 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & -1 & 0 & 0 & \ldots & 0 \end{vmatrix}.$$

Appliquant une fois de plus le théorème de Laplace, développons ce déterminant par rapport aux mineurs extraits des n dernières colonnes. Le mineur complémentaire du mineur $|C|$ est égal à $(-1)^n$; le mineur $|C|$ étant engendré par les n premières lignes et les n dernières colonnes et vu que

$$1+2+\ldots+n+(n+1)+(n+2)+\ldots+2n = 2n^2+n,$$

il vient

$$\Delta = (-1)^{2n^2+n}(-1)^n|C| = (-1)^{2(n^2+n)}|C|$$

ou encore

$$\Delta = |C|, \tag{5}$$

car le nombre $2(n^2+n)$ est pair.

Enfin de (4) et (5) découle l'égalité que nous voulons démontrer:

$$|C| = |A|\cdot|B|.$$

On aurait pu démontrer le théorème de la multiplication des déterminants sans utiliser le théorème de Laplace. Le lecteur trouvera l'une des démonstrations de ce genre à la fin du § 16.

§ 14. Matrice inverse

Une matrice carrée est dite *dégénérée* ou *singulière* si son déterminant est nul, sinon elle est dite *non dégénérée* ou *non singulière*. D'une façon analogue, une transformation linéaire des indéterminées est dite *singulière* (dégénérée) ou *non singulière* (non dégénérée) selon que le déterminant de ses coefficients est nul ou non nul. La proposition suivante résulte du théorème démontré à la fin du paragraphe précédent.

Le produit d'un nombre quelconque de matrices est une matrice singulière si au moins un des facteurs est une matrice singulière.

Le produit d'un nombre arbitraire de matrices non singulières est une matrice non singulière.

Etant donné la relation qui existe entre la multiplication des matrices et le résultat de l'application successive de transformations linéaires, il découle de cette proposition la proposition analogue pour les transformations linéaires: *pour que le résultat de l'application successive d'un certain nombre de transformations linéaires soit une transformation linéaire non singulière, il faut et il suffit que toutes les transformations données soient non singulières.*

C'est la matrice

$$E=\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & . & . & . \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

qui joue le rôle d'unité dans la multiplication des matrices. En outre, E commute avec toute matrice A du même ordre que E:

$$AE=EA=A. \tag{1}$$

On démontre ces égalités soit en appliquant directement les règles de multiplication des matrices, soit en s'appuyant sur le fait que la matrice unité E correspond à la transformation linéaire *identique* des indéterminées

$$\begin{aligned} x_1 &= y_1, \\ x_2 &= y_2, \\ &\dots \\ x_n &= y_n; \end{aligned}$$

il est clair que la transformation identique appliquée avant ou après une transformation donnée ne change pas cette dernière.

Notons que la *matrice E est la seule matrice qui satisfasse à la condition* (1) *pour toute matrice A*. En effet, supposons qu'il existe une autre matrice E' ayant la même propriété. Ceci étant, on a

$$E'E=E', \qquad E'E=E,$$

d'où $E'=E$.

L'existence pour une matrice donnée A de la *matrice inverse* est déjà un problème plus compliqué. La multiplication des matrices étant non commutative, nous allons considérer d'abord l'inverse *à droite* d'une matrice, c'est-à-dire une matrice A^{-1} telle que la multiplication à droite de la matrice A par cette matrice donne

la matrice unité pour produit:

$$AA^{-1} = E. \tag{2}$$

Supposons que la matrice A soit singulière et que la matrice A^{-1}, ayant la propriété (2), existe. Alors le premier membre de la relation (2), comme on le sait déjà, est une matrice singulière tandis que le second membre de (2) est une matrice non singulière, son déterminant étant égal à l'unité. Ainsi, la matrice singulière ne peut pas avoir de matrice inverse à droite. Les mêmes considérations montrent qu'elle ne possède pas non plus de matrice inverse à gauche, de sorte qu'*une matrice singulière n'a pas de matrice inverse.*

Passant maintenant au cas d'une matrice non singulière, introduisons d'abord une notion auxiliaire. Soit une matrice d'ordre n:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

La matrice

$$A^* = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \cdot & \cdot & \cdot & \cdot \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix},$$

dont l'élément appartenant à la $j^{\text{ème}}$ ligne et à la $i^{\text{ème}}$ colonne est le cofacteur de l'élément a_{ij} dans la matrice A, est dite matrice *adjointe* de la matrice A.

Calculons les produits AA^* et A^*A. Utilisant la formule du § 6 sur le développement d'un déterminant par rapport aux éléments d'une de ses lignes ou d'une de ses colonnes, ainsi que le théorème du § 7 sur la somme des produits des éléments d'une ligne (ou colonne) d'un déterminant par les cofacteurs des éléments correspondants d'une autre ligne (ou colonne), nous obtenons, en désignant par d le déterminant de la matrice A

$$d = |A|,$$

les égalités suivantes

$$AA^* = A^*A = \begin{pmatrix} d & 0 & \dots & 0 \\ 0 & d & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & d \end{pmatrix}. \tag{3}$$

Il en résulte que *si la matrice A est non singulière, alors sa matrice adjointe A^* l'est aussi et le déterminant d^* de celle-ci est égal au déterminant d de la matrice A élevé à la puissance* $(n-1)$.

En effet, passant des égalités (3) aux égalités correspondantes pour les déterminants, il vient

$$dd^* = d^n,$$

d'où, vu que $d \neq 0$, il vient encore

$$d^* = d^{n-1}\,[1].$$

A présent il est facile de démontrer l'existence de la matrice inverse pour toute matrice *non singulière A* et trouver cette matrice inverse. Notons d'abord qu'en divisant tous les éléments d'un des facteurs du produit AB, par exemple, tous les éléments de B, par un même nombre d, tous les éléments du produit AB se trouvent divisés par ce nombre. Pour le démontrer, il suffit de rappeler la définition de la multiplication des matrices. Ainsi, si

$$d = |A| \neq 0,$$

alors on déduit des égalités (3) la formule pour la matrice inverse A^{-1}:

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{d} & \frac{A_{21}}{d} & \ldots & \frac{A_{n1}}{d} \\ \frac{A_{12}}{d} & \frac{A_{22}}{d} & \ldots & \frac{A_{n2}}{d} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{A_{1n}}{d} & \frac{A_{2n}}{d} & \ldots & \frac{A_{nn}}{d} \end{pmatrix}.$$

Autrement dit, *l'inverse d'une matrice A s'obtient en divisant tous les éléments de la matrice adjointe A^* par le nombre d*. En effet, les égalités (3) donnent immédiatement

$$AA^{-1} = A^{-1}A = E. \qquad (4)$$

Notons, une fois de plus, que la $i^{\text{ème}}$ *ligne* de la matrice A^{-1} a pour éléments les cofacteurs des éléments correspondants de la $i^{\text{ème}}$ *colonne* du déterminant $|A|$ divisés par $d = |A|$.

Il est facile de démontrer que *toute matrice A non singulière possède une seule matrice A^{-1} satisfaisant à la condition* (4). En effet, soit C une autre matrice telle que

$$AC = CA = E.$$

---

[1] On pourrait montrer que, la matrice A étant dégénérée, il en est de même de la matrice adjointe A^* ; en outre, dans ce cas le rang de A^* n'est pas supérieur à l'unité.

Alors il s'ensuit de ces égalités

$$CAA^{-1} = C(AA^{-1}) = CE = C,$$
$$CAA^{-1} = (CA)A^{-1} = EA^{-1} = A^{-1},$$

d'où $C = A^{-1}$.

Le théorème de la multiplication des déterminants et les relations (4) montrent que le *déterminant de la matrice A^{-1} est égal à $\frac{1}{|A|}$, de sorte que A^{-1} est également non singulière*; *évidemment, l'inverse de la matrice A^{-1} est la matrice A.*

Soient à présent A et B deux matrices carrées d'ordre n, A non singulière et B quelconque. A étant non singulière, nous pouvons *diviser la matrice B par la matrice A* respectivement *à droite et à gauche*, en d'autres termes nous sommes en mesure de résoudre les équations matricielles

$$AX = B, \qquad YA = B. \tag{5}$$

Pour cela, il suffit, en vertu de l'associativité de la multiplication des matrices, de poser

$$X = A^{-1}B, \qquad Y = BA^{-1};$$

en outre, ces solutions des équations (5) sont, dans le cas général, des matrices distinctes, vu que la multiplication des matrices est non commutative.

Exemples. 1) Soit la matrice

$$A = \begin{pmatrix} 3 & -1 & 0 \\ -2 & 1 & 1 \\ 2 & -1 & 4 \end{pmatrix}.$$

Son déterminant étant 5, la matrice inverse A^{-1} existe et est de la forme

$$A^{-1} = \begin{pmatrix} 1 & \frac{4}{5} & -\frac{1}{5} \\ 2 & \frac{12}{5} & -\frac{3}{5} \\ 0 & \frac{1}{5} & \frac{1}{5} \end{pmatrix}.$$

2) Soient deux matrices

$$A = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 7 \\ 3 & 5 \end{pmatrix}.$$

La matrice A étant non singulière, la matrice A^{-1} existe et est de la forme

$$A^{-1} = \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix},$$

de sorte que les solutions des équations matricielles $AX=B$, $YA=B$ sont respectivement les matrices

$$X=\begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix}\cdot\begin{pmatrix} -1 & 7 \\ 3 & 5 \end{pmatrix}=\begin{pmatrix} -9 & 11 \\ 13 & -13 \end{pmatrix},$$

$$Y=\begin{pmatrix} -1 & 7 \\ 3 & 5 \end{pmatrix}\cdot\begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix}=\begin{pmatrix} -31 & 23 \\ -11 & 9 \end{pmatrix}.$$

Multiplication des matrices rectangulaires. Bien que la multiplication des matrices que nous venons d'introduire dans le paragraphe précédent ne soit définie jusqu'ici que pour les matrices carrées d'un même ordre, on peut généraliser cette opération algébrique de manière qu'elle soit applicable dans le cas des matrices rectangulaires A et B, à condition, toutefois, que la formule (3) du paragraphe précédent ait un sens, c'est-à-dire à condition que toute ligne de A contienne le même nombre d'éléments que toute colonne de la matrice B. En d'autres termes, *on peut parler du produit des matrices rectangulaires A et B si et seulement si le nombre des colonnes de la matrice A est égal au nombre des lignes de la matrice B ; en outre, le nombre des lignes de la matrice AB est égal à celui des lignes de la matrice A et le nombre des colonnes de la matrice AB à celui des colonnes de la matrice B.*

Exemples.

1) $$\begin{pmatrix} 5 & -1 & 3 & 1 \\ 2 & 0 & -1 & 4 \end{pmatrix}\cdot\begin{pmatrix} -1 & 3 & 0 \\ -2 & 1 & 1 \\ 3 & 0 & -2 \\ 4 & 1 & 2 \end{pmatrix}=\begin{pmatrix} 10 & 15 & -5 \\ 11 & 10 & 10 \end{pmatrix}.$$

2) $$\begin{pmatrix} 0 & -3 & 1 \\ 2 & 1 & 5 \\ -4 & 0 & -2 \end{pmatrix}\cdot\begin{pmatrix} 3 \\ -2 \\ 2 \end{pmatrix}=\begin{pmatrix} 8 \\ 14 \\ -16 \end{pmatrix}$$

3) $$(5\ 1\ 0\ -3)\cdot\begin{pmatrix} 2 & 0 \\ 1 & -4 \\ 3 & 1 \\ 0 & -1 \end{pmatrix}=(11\ -1).$$

On peut établir la relation qui existe entre la multiplication des matrices rectangulaires et le produit des transformations linéaires des indéterminées, à condition, toutefois, que dans la définition des transformations linéaires on renonce à l'hypothèse que le nombre des indéterminées soit conservé.

Il est facile de vérifier, en répétant sans modification aucune la démonstration donnée ci-dessus, dans le cas des matrices carrées, que la *loi d'associativité est valable pour la multiplication des matrices rectangulaires.*

Nous allons utiliser la multiplication des matrices rectangulaires et les propriétés de la matrice inverse pour donner une *nouvelle démonstration des formules de Cramer*, cette démonstration ne nécessitant pas les calculs laborieux qui ont été faits au § 7. Soit un système cramérien de n équations linéaires à n inconnues, c'est-à-dire un système dont le déterminant n'est pas nul:

$$\left.\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = b_n. \end{array}\right\} \quad (6)$$

Notons par A la matrice des coefficients du système (6); en vertu de notre hypothèse ($d = |A| \neq 0$), la matrice A est non singulière. Désignons respectivement par X et B les colonnes des inconnues et des seconds membres du système (6), à savoir

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Le nombre des colonnes de la matrice A étant égal à celui des lignes de la matrice X, le produit AX a un sens et est égal à la colonne des premiers membres des équations (6). Ainsi, le système (6) peut être récrit sous la forme d'une équation matricielle:

$$AX = B. \quad (7)$$

La matrice A étant non singulière, son inverse A^{-1} existe; multipliant à gauche les deux membres de l'équation (7) par A^{-1}, il vient:

$$X = A^{-1}B. \quad (8)$$

Le produit $A^{-1}B$ est une matrice colonne; son $j^{\text{ème}}$ élément est égal à la somme des produits des éléments de la $j^{\text{ème}}$ ligne de la matrice A^{-1} par les éléments correspondants de la matrice B, c'est-à-dire qu'il est égal à

$$\frac{A_{1j}}{d} b_1 + \frac{A_{2j}}{d} b_2 + \ldots + \frac{A_{nj}}{d} b_n = \frac{1}{d}(A_{1j}b_1 + A_{2j}b_2 + \ldots + A_{nj}b_n).$$

Or, l'expression entre parenthèses dans le second membre n'est autre que le développement, par rapport aux éléments de la $j^{\text{ème}}$ colonne, du déterminant d_j qui s'obtient du déterminant d en remplaçant sa $j^{\text{ème}}$ colonne par la colonne B. Ainsi, les formules (8) coïncident avec les formules (3) du § 7 qui sont exactement celles de Cramer pour la solution du système (6).

Il reste à montrer que l'expression (8) est effectivement la solution de (6). Pour cela, il suffit de remplacer dans (7) la matrice colonne X par son expression (8), ce qui conduit immédiatement à l'identité $B = B$.

Rang du produit de matrices. Le théorème de la multiplication des déterminants donne dans le cas des matrices singulières que leur produit est aussi une matrice singulière, mais ne permet pas de préciser quel sera le rang de ce produit. Pourtant, il est naturel de classer les matrices carrées singulières d'après leur rang. Notons qu'il n'existe pas de relation bien déterminée entre les rangs des facteurs et celui du produit, comme le montrent les exemples suivants:

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};$$

dans ces deux cas on multiplie des matrices de rang 1, le produit est de rang 1 dans le premier cas et de rang 0 dans le second. Néanmoins, on peut énoncer le théorème suivant qui est valable non seulement pour les matrices carrées, mais aussi pour les matrices rectangulaires.

Le rang du produit de matrices n'est pas supérieur au rang de chaque facteur.

Il suffit de démontrer ce théorème dans le cas de deux facteurs. Soient A et B deux matrices, le produit AB ayant un sens; notons ce produit par C: $AB = C$. Revenons à la formule (3) du § 13 et exprimons les éléments de la matrice C par les éléments des A et B. Fixant dans cette formule l'entier k et faisant varier l'entier i ($i = 1, 2, \ldots, n$), on constate que la $k^{\text{ème}}$ colonne de la matrice C est une combinaison linéaire, avec certains coefficients (à savoir les coefficients $b_{1k}, b_{2k}, \ldots$), des colonnes de la matrice A. Cela prouve que le système des colonnes de la matrice C s'exprime linéairement par le système des colonnes de la matrice A, de sorte que le rang du premier système est inférieur ou égal à celui du second, en vertu du résultat correspondant du § 9; en d'autres termes, le rang de la matrice C n'est pas supérieur à celui de la matrice A. Comme, d'autre part, la même formule (3) du § 13 montre (pour i fixé et k variant entre 1 et n) que la $i^{\text{ème}}$ ligne de la matrice C est une combinaison linéaire des lignes de la matrice B, les raisonnements analogues prouvent que le rang de C ne peut être supérieur à celui de B.

On a un résultat plus précis lorsqu'un des facteurs est une matrice carrée non singulière.

Le rang des produits AQ et QA, où A est quelconque et Q une matrice carrée non singulière, est égal au rang de A.

Montrons-le, par exemple, pour le produit

$$AQ = C. \tag{9}$$

Il s'ensuit du théorème précédent que le rang de la matrice C est inférieur ou égal à celui de la matrice A. Multipliant à droite les deux membres de (9) par Q^{-1}, nous sommes conduits à l'égalité

$$A = CQ^{-1},$$

de sorte qu'en vertu du même théorème, le rang de A n'est pas supérieur à celui de C. Ces deux résultats démontrent que les rangs de A et de C coïncident.

§ 15. Addition des matrices et multiplication des matrices par un nombre

Pour les matrices carrées d'ordre n on définit l'*addition* de la manière suivante:

On appelle *somme de deux matrices carrées d'ordre n $A = (a_{ij})$ et $B = (b_{ij})$, et on la note par $A + B$,* une matrice $C = (c_{ij})$ telle que tout élément de C est la somme des éléments correspondants des matrices A et B:

$$c_{ij} = a_{ij} + b_{ij}\ ^{1}.$$

Il est clair que l'addition des matrices ainsi définie est commutative et associative. L'opération inverse, dite soustraction, est bien définie: la différence de deux matrices A et B est une matrice dont les éléments sont les différences des éléments correspondants des matrices données. Le rôle de l'élément nul est joué par la *matrice nulle* dont tous les éléments sont nuls; dans tout ce qui suit cette matrice sera notée par le symbole 0; il n'y a pas de danger sérieux de confondre la matrice nulle avec le nombre zéro.

L'addition des matrices carrées et leur multiplication définie au § 13 sont liées par la loi de distributivité.

En effet, soient $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ trois matrices d'ordre n. Alors, pour i et j quelconques on a l'égalité évidente

$$\sum_{s=1}^{n} (a_{is} + b_{is})\, c_{sj} = \sum_{s=1}^{n} a_{is}c_{sj} + \sum_{s=1}^{n} b_{is}c_{sj}.$$

[1] Bien entendu, on aurait pu définir la multiplication des matrices de la manière aussi naturelle que leur addition, en posant l'élément générique du produit des matrices égal au produit des éléments correspondants des matrices facteurs. Toutefois, une telle multiplication, différemment de celle introduite dans le § 13, ne trouverait pas d'applications utiles.

Or, le premier membre de cette égalité est l'élément qui se trouve à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne de la matrice $(A + B)\,C$, tandis que le second membre est l'élément qui occupe la même place dans la matrice $AC + BC$. Ceci démontre l'identité

$$(A+B)\,C = AC + BC.$$

La relation $C\,(A + B) = CA + CB$ se démontre de la même manière, la non-commutativité de la multiplication des matrices nécessitant, évidemment, la démonstration des deux lois de distributivité.

Définissons maintenant la multiplication d'une matrice par un nombre.

On appelle *produit d'une matrice carrée* $A = (a_{ij})$ *par un nombre* k *et on le note* kA une matrice $A' = (a'_{ij})$ qui s'obtient de la matrice A en multipliant tous ses éléments par k, à savoir:

$$a'_{ij} = ka_{ij}.$$

Nous avons déjà eu à faire dans le paragraphe précédent à un exemple de la multiplication de ce genre: l'inverse A^{-1} et la matrice adjointe A^* d'une matrice A non singulière sont liées par la relation

$$A^{-1} = d^{-1}A^*,$$

où d est le déterminant de A.

Nous savons déjà que toute matrice carrée d'ordre n peut être considérée comme un vecteur à n^2 dimensions; en outre, il y a une correspondance bijective entre les matrices carrées d'ordre n et les vecteurs à n^2 composantes. L'addition des matrices et leur multiplication par un nombre, que nous avons définies, se transforment en addition des vecteurs et multiplication des vecteurs par un nombre de l'espace vectoriel à n^2 dimensions. Par conséquent, *l'ensemble des matrices carrées d'ordre* n *peut être considéré comme un espace vectoriel à* n^2 *dimensions.*

Il en résulte les égalités

$$k\,(A+B) = kA + kB, \tag{1}$$

$$(k+l)\,A = kA + lA, \tag{2}$$

$$k\,(lA) = (kl)\,A, \tag{3}$$

$$1 \cdot A = A, \tag{4}$$

où A et B sont des matrices d'ordre n, k et l des nombres quelconques et le signe 1 désigne le nombre un.

Les propriétés (1) et (2) relient la multiplication d'une matrice par un nombre et l'addition des matrices. Il existe également une relation très importante entre la multiplication d'une matrice par

un nombre et la multiplication des matrices, à savoir:

$$(kA)\,B = A\,(kB) = k\,(AB)\,; \tag{5}$$

autrement dit, *multipliant dans un produit de matrices un des facteurs par le nombre k, le produit se trouve multiplié par ce même nombre k.*

En effet, soient $A = (a_{ij})$ et $B = (b_{ij})$ deux matrices et k un nombre quelconque. Alors on a:

$$\sum_{s=1}^{n} (ka_{is})\,b_{sj} = k \sum_{s=1}^{n} a_{is}b_{sj},$$

quels que soient les entiers i et j, $i, j = 1, 2, \ldots, n$. Or, le premier membre de cette égalité est l'élément qui se trouve à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne de la matrice $(kA)\,B$, tandis que son second membre est l'élément qui occupe la même place dans la matrice $k\,(AB)$. Ceci démontre l'identité

$$(kA)\,B = k\,(AB).$$

L'égalité $A\,(kB) = k\,(AB)$ se démontre de la même manière.

La multiplication d'une matrice par un nombre permet d'introduire une nouvelle écriture pour les matrices. On notera E_{ij} la matrice dont l'élément qui se trouve à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne est l'unité et tous les autres éléments sont nuls. Faisant $i, j = 1, 2, \ldots, n$, on obtient n^2 matrices E_{ij} qui vérifient, comme il est facile de constater, la table de multiplication:

$$E_{is}E_{sj} = E_{ij}, \qquad E_{is}E_{tj} = 0 \quad \text{pour} \quad s \neq t.$$

L'élément qui se trouve à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne de la matrice kE_{ij} est le nombre k; c'est la seule différence qu'il y ait entre les matrices kE_{ij} et E_{ij}. Tenant compte de ce fait et utilisant la définition de l'addition des matrices, on obtient une nouvelle représentation d'une matrice carrée A:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}E_{ij}\,; \tag{6}$$

en outre, toute matrice A peut être représentée d'une façon unique sous la forme (6).

D'après la définition de la multiplication d'une matrice par un nombre, la matrice kE, où E est la matrice unité, est de la forme:

$$kE = \begin{pmatrix} k & & & 0 \\ & k & & \\ & & \ddots & \\ 0 & & & k \end{pmatrix},$$

c'est-à-dire que tous les éléments de la diagonale principale de cette matrice sont égaux à k, tandis que tous les autres éléments sont nuls. Les matrices de cette forme sont dites *scalaires*.

La définition de l'addition des matrices nous conduit à l'égalité

$$kE + lE = (k + l)\,E. \tag{7}$$

D'autre part, utilisant la définition de la multiplication des matrices ou s'appuyant sur l'égalité (5), on obtient :

$$kE \cdot lE = (kl)\,E. \tag{8}$$

La multiplication d'une matrice A par un nombre k peut être interprétée comme la multiplication de A par la matrice scalaire kE dans le sens de la multiplication des matrices. En effet, d'après (5), on a

$$(kE)\,A = A\,(kE) = kA.$$

Il en découle que *toute matrice scalaire commute avec toute matrice A*. Il est très important de souligner que les matrices scalaires sont les seules à jouir de cette propriété :

Si une matrice $C = (c_{ij})$ d'ordre n commute avec toutes les matrices de même ordre, alors C est scalaire.

En effet, soit $i \neq j$ et considérons les matrices CE_{ij} et $E_{ij}C$; en vertu de notre hypothèse, $CE_{ij} = E_{ij}C$ (cf. la définition ci-dessus de la matrice E_{ij}). Il est facile de voir que toutes les colonnes de la matrice CE_{ij}, excepté la $j^{\text{ème}}$, sont composées d'éléments nuls, tandis que la $j^{\text{ème}}$ colonne de ce produit coïncide avec la $i^{\text{ème}}$ colonne de la matrice C ; en particulier, à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne de la matrice CE_{ij} se trouve l'élément c_{ii}. De façon analogue, toutes les lignes de la matrice $E_{ij}C$, excepté la $i^{\text{ème}}$, ont pour éléments l'élément nul, tandis que la $i^{\text{ème}}$ ligne de ce produit coïncide avec la $j^{\text{ème}}$ ligne de la matrice C ; à l'intersection de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne de la matrice $E_{ij}C$ se trouve l'élément c_{jj}. En vertu de l'égalité $CE_{ij} = E_{ij}C$, on a $c_{ii} = c_{jj}$ (en tant qu'éléments occupant les mêmes places dans les matrices égales), c'est-à-dire la diagonale principale de la matrice C a pour éléments un même nombre. D'autre part, à l'intersection de la $j^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne de la matrice CE_{ij} se trouve l'élément c_{ji} tandis que dans la matrice $E_{ij}C$ la même place est occupée par l'élément nul (car $i \neq j$), de sorte que $c_{ji} = 0$, ou, encore, tout élément de la matrice C se trouvant en dehors de la diagonale principale est nul. Le théorème est démontré.

§ 16*. Théorie axiomatique des déterminants

Un déterminant d'ordre n est un nombre bien défini par la matrice carrée d'ordre n associée. La définition de ce nombre donnée au § 4 indique une règle selon laquelle le déterminant s'exprime

par les éléments de la matrice associée. Cette définition constructive peut être remplacée par une définition axiomatique ; en d'autres termes, on peut trouver, parmi les propriétés des déterminants établies aux §§ 4 et 6, celles qui les caractérisent complètement, de sorte que la seule fonction d'une matrice à valeurs réelles vérifiant ces propriétés soit son déterminant.

On peut utiliser le développement d'un déterminant par rapport aux éléments d'une ligne pour donner une des définitions de ce genre. Considérons l'ensemble des matrices carrées d'un ordre quelconque et supposons qu'à toute matrice M corresponde un nombre d_M vérifiant les conditions suivantes :

1) Si une matrice M est d'ordre un, c'est-à-dire M ne contient qu'un seul élément a, alors $d_M = a$.

2) Soient $a_{11}, a_{12}, \ldots, a_{1n}$ les éléments de la première ligne de la matrice M d'ordre n et soit M_i la matrice d'ordre $n-1$ qui s'obtient de la matrice M en supprimant sa première ligne et sa $i^{\text{ème}}$ colonne, $i = 1, 2, \ldots, n$; alors

$$d_M = a_{11}d_{M_1} - a_{12}d_{M_2} + a_{13}d_{M_3} - \ldots + (-1)^{n-1} a_{1n}d_{M_n}.$$

Alors pour chaque matrice M le nombre d_M est égal au déterminant de cette matrice. Nous laissons au lecteur le soin de vérifier cette proposition, sa démonstration se faisant par récurrence sur n et utilisant les résultats du § 6.

Beaucoup plus d'intérêt comportent d'autres formes axiomatiques de la définition des déterminants se rapportant au cas où n est fixé et s'appuyant sur quelques propriétés simples des déterminants établies au § 4. Nous passons maintenant à l'une de ces définitions.

Supposons qu'à toute matrice carrée M d'ordre n corresponde un nombre d_M vérifiant les conditions suivantes :

I. *Si on multiplie l'une des lignes de la matrice M par un nombre k, alors le nombre d_M est multiplié par k.*

II. *Le nombre d_M est conservé lorsqu'on ajoute à l'une des lignes de la matrice M une autre ligne de cette matrice.*

III. *Si E est la matrice unité, alors $d_E = 1$.*

Montrons que pour *toute matrice M le nombre d_M est égal à son déterminant.*

Déduisons d'abord des conditions I-III certaines propriétés du nombre d_M qui sont analogues aux propriétés correspondantes du déterminant.

(1) *Si l'une des lignes de la matrice M est composée d'éléments nuls, alors $d_M = 0$.*

En effet, multipliant la ligne composée de zéros par le nombre 0, la matrice M ne change pas tandis que le nombre d_M, en vertu de la condition I, se trouve multiplié par 0, de sorte que

$$d_M = 0 \cdot d_M = 0.$$

(2) *Le nombre* d_M *est conservé lorsqu'on ajoute à la* $i^{\text{ème}}$ *ligne de la matrice* M *sa* $j^{\text{ème}}$ *ligne multipliée par un nombre* k $(i \neq j)$.

Pour $k = 0$ la proposition est évidente. Soit $k \neq 0$. Multipliant la $j^{\text{ème}}$ ligne par k nous obtenons une matrice M' pour laquelle, en vertu de I, on a $d_{M'} = kd_M$. Ajoutant ensuite à la $i^{\text{ème}}$ ligne de la matrice M' sa $j^{\text{ème}}$ ligne nous obtenons une matrice M'' telle que $d_{M''} = d_{M'}$, en vertu de la condition II. Enfin, multipliant la $j^{\text{ème}}$ ligne de la matrice M'' par le nombre k^{-1}, nous avons une matrice M''' qui s'obtient de la matrice M par la transformation indiquée dans l'énoncé de la propriété (2); en outre

$$d_{M'''} = k^{-1}d_{M''} = k^{-1}d_{M'} = k^{-1} \cdot kd_M = d_M.$$

(3) *Si les lignes de la matrice* M *sont linéairement dépendantes, alors* $d_M = 0$.

En effet, supposons que la $i^{\text{ème}}$ ligne soit une combinaison linéaire des autres lignes. Appliquant à la matrice M la transformation (2) et réitérant ce procédé on peut remplacer les éléments de la $i^{\text{ème}}$ ligne de M par l'élément nul. La transformation (2) conserve le nombre d_M et, vu la propriété (1), il vient $d_M = 0$.

(4) *Supposons que la* $i^{\text{ème}}$ *ligne de la matrice* M *soit la somme de deux vecteurs* β *et* γ *et soient* M' *et* M'' *les matrices qui s'obtiennent de la matrice* M *en remplaçant sa* $i^{\text{ème}}$ *ligne respectivement par les vecteurs* β *et* γ. *Alors*

$$d_M = d_{M'} + d_{M''}.$$

En effet, désignons par S la famille de toutes les lignes de la matrice M, excepté la $i^{\text{ème}}$. Si la famille S est non libre, alors il en est de même pour les lignes de chacune des matrices M, M' et M'', de sorte qu'en vertu de la propriété (3), on a $d_M = d_{M'} = d_{M''} = 0$, d'où la proposition (4). Si, par contre, la famille S, composée de $n - 1$ vecteurs, est libre, on peut alors la compléter par un vecteur, soit α, de telle manière qu'elle devienne maximale dans un espace vectoriel à n dimensions, comme le montrent les résultats du § 9. Les vecteurs β et γ s'expriment par les vecteurs de cette famille maximale. Supposons que le vecteur α intervienne dans les expressions de β et γ respectivement avec les coefficients k et l; par conséquent, le vecteur α intervient dans l'expression du vecteur $\beta + \gamma$ (qui n'est autre que la $i^{\text{ème}}$ ligne de la matrice M) avec le coefficient $k + l$. Retranchant des $i^{\text{èmes}}$ lignes des matrices M, M' et M'' des combinaisons linéaires des autres lignes, on peut transformer ces matrices de manière que leurs $i^{\text{èmes}}$ lignes deviennent respectivement les vecteurs $(k + l)\,\alpha$, $k\alpha$, $l\alpha$. Ainsi, notant par M^0 la matrice qui s'obtient en remplaçant la $i^{\text{ème}}$ ligne de la matrice M par le vecteur α et compte tenu des propriétés (2) et I, nous avons les

égalités:

$$d_M = (k+l)\, d_{M^0}, \quad d_{M'} = k d_{M^0}, \quad d_{M''} = l d_{M^0}.$$

La propriété (4) est donc démontrée.

(5) *A la matrice $\overline{M}$, qui s'obtient de la matrice M en transposant deux lignes quelconques, correspond le nombre $d_{\overline{M}} = -d_M$.*

En effet, supposons qu'on doive permuter les lignes d'indices i et j de la matrice M. On y arrive en appliquant successivement les transformations suivantes: on ajoute d'abord à la $i^{\text{ème}}$ ligne de la matrice M sa $j^{\text{ème}}$ ligne et on obtient une matrice, notée M', telle que $d_{M'} = d_M$, en vertu de la condition II. Retranchant ensuite de la $j^{\text{ème}}$ ligne de la matrice M' sa $i^{\text{ème}}$ ligne nous avons une matrice M'' pour laquelle, en vertu de la propriété (2), on a encore $d_{M''} = d_{M'}$; les éléments de la $j^{\text{ème}}$ ligne de la matrice M'' diffèrent par leur signe des éléments correspondants de la $i^{\text{ème}}$ ligne de la matrice M. Ajoutant maintenant à la $i^{\text{ème}}$ ligne de la matrice M'' sa $j^{\text{ème}}$ ligne, on obtient une matrice M''' telle que $d_{M'''} = d_{M''}$, en vertu de la condition II. En outre, la $i^{\text{ème}}$ ligne de M''' coïncide avec la $j^{\text{ème}}$ ligne de M. Multipliant, enfin, la $j^{\text{ème}}$ ligne de la matrice M''' par le nombre -1, nous obtenons la matrice $\overline{M}$ dont il est question dans l'énoncé de la propriété (5). En vertu de la condition I, on a

$$d_{\overline{M}} = -d_{M'''} = -d_M.$$

(6) *Si la matrice M' s'obtient de la matrice M en permutant des lignes de M (la $i^{\text{ème}}$ ligne de la matrice M' étant la $\alpha_i^{\text{ème}}$ ligne de la matrice M, $i = 1, 2, \ldots, n$), alors*

$$d_{M'} = \pm d_M;$$

le signe plus correspond au cas où la substitution

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}$$

est paire et le signe moins au cas où elle est impaire.

En effet, la matrice M' peut être obtenue de la matrice M par plusieurs transpositions de deux lignes, de sorte que nous pouvons appliquer la propriété (5). La parité du nombre de ces transpositions, comme on le sait du § 3, détermine la parité de la substitution en question.

Considérons à présent les matrices $M = (a_{ij})$, $N = (b_{ij})$ et formons leur produit $Q = MN$ au sens du § 13. Calculons le nombre d_Q correspondant. On sait que la $i^{\text{ème}}$ ligne de la matrice Q est la combinaison linéaire des lignes de la matrice N respectivement de coefficients $a_{i1}, a_{i2}, \ldots, a_{in}$ et ceci pour tous les i, $i = 1, 2, \ldots$

. . ., n (cf. par exemple § 14). Substituons aux lignes de la matrice Q leurs expressions linéaires par les lignes de la matrice N et appliquons plusieurs fois la propriété (4). Nous constatons que le nombre d_Q est égal à la somme des nombres d_T, correspondant à toutes les matrices T de la forme suivante : la $i^{\text{ème}}$ ligne de la matrice T coïncide avec la $\alpha_i^{\text{ème}}$ ligne de la matrice N multipliée par le nombre $a_{i\alpha_i}$ et cela pour tous les i, $i = 1, 2, \ldots, n$. En outre, d'après la propriété (3), on peut omettre toutes les matrices T pour lesquelles il existe des indices i et j tels que $\alpha_i = \alpha_j$ avec $i \neq j$; autrement dit, nous ne devons conserver que les matrices T pour lesquelles les indices $\alpha_1, \alpha_2, \ldots, \alpha_n$ correspondants forment une permutation des nombres $1, 2, \ldots, n$. Le nombre d_T, pour une telle matrice T, en vertu des propriétés I et (6), est de la forme

$$d_T = \pm a_{1\alpha_1} a_{2\alpha_2} \ldots a_{n\alpha_n} d_N,$$

le signe du second membre étant défini par la parité de la permutation des indices. Ceci nous conduit à l'expression du nombre d_Q que nous nous sommes proposé de calculer : mettant en facteur le nombre d_N, commun à tous les termes de la somme exprimant d_Q, on obtient évidemment pour second facteur le déterminant $|M|$ de la matrice M au sens de la définition constructive du § 4. Ainsi

$$d_Q = |M| \cdot d_N. \qquad (*)$$

Prenant dans (*) pour matrice N la matrice unité E, il vient : $Q = M$ et, en même temps, d'après la propriété III, $d_N = d_E = 1$, c'est-à-dire *pour toute matrice M on a l'égalité suivante* :

$$d_M = |M|,$$

ce qu'il fallait démontrer. *Nous avons donné en même temps une nouvelle démonstration du théorème de la multiplication des déterminants sans utiliser le théorème de Laplace* : pour cela il suffit de remplacer dans l'égalité (*) les nombres d_Q et d_N par les déterminants des matrices correspondantes.

Nous terminerons ces considérations axiomatiques en démontrant l'*indépendance* des conditions I-III, en d'autres termes, nous allons montrer qu'aucune de ces conditions n'est la conséquence des deux autres.

Pour démontrer l'indépendance de la condition III, posons pour toute matrice M d'ordre n : $d_M = 0$. Les conditions I et II sont, évidemment, vérifiées, tandis que la condition III n'a plus lieu.

Pour démontrer l'indépendance de la condition II, posons pour toute matrice M le nombre d_M égal au produit des éléments de la diagonale principale de M. Les conditions I et III sont encore valables, tandis que la condition II n'a pas lieu.

Enfin, pour démontrer l'indépendance de la condition I, posons : $d_M = 1$ pour toute matrice M. Les conditions II et III sont toujours valables, tandis que la condition I n'a plus lieu.

Chapitre IV | **NOMBRES COMPLEXES**

§ 17. Ensemble des nombres complexes

L'étude suivie de l'algèbre élémentaire conduit progressivement à la généralisation de la notion de nombre. Un écolier qui aborde le cours d'algèbre part des notions de nombres entiers et fractionnaires positifs qui lui ont été enseignées en arithmétique. En substance l'algèbre élémentaire commence par l'introduction des *nombres entiers* négatifs, c'est-à-dire par l'introduction du système numérique des nombres entiers composé d'entiers positifs, négatifs et de zéro. Puis vient le tour des *nombres rationnels*, positifs et négatifs, qui constituent déjà un ensemble assez riche.

On étend encore la notion de nombre en complétant l'ensemble des nombres rationnels par les nombres irrationnels. Les nombres rationnels et irrationnels constituent l'ensemble des *nombres réels*. Les fondements mathématiques rigoureux de la théorie des nombres réels sont l'objet de l'étude systématique du cours universitaire d'analyse; néanmoins, la notion de nombre réel acquise à l'école secondaire suffit largement pour aborder l'étude de l'algèbre supérieure.

Finalement, en fin du cours d'algèbre élémentaire on enseigne les *nombres complexes*, généralisant les nombres réels. Le lecteur qui n'a pas eu assez de temps pour se familiariser avec l'ensemble des nombres complexes aura sûrement besoin d'une étude plus détaillée de ces nombres, d'autant plus qu'ils jouissent de nombreuses bonnes propriétés. C'est pourquoi ce chapitre sera consacré à une étude assez complète des nombres complexes.

On est obligé d'introduire les nombres complexes lorsqu'on considère le problème de résolution d'une équation du second degré à coefficients réels. On sait que les nombres réels ne suffisent pas pour qu'on puisse trouver les racines de toute équation de ce type. La plus simple équation du second degré n'ayant pas de racines réelles est

$$x^2+1=0. \tag{1}$$

Il s'agit de généraliser la notion de nombre réel en introduisant un ensemble de nombres plus riche de telle manière que l'équation (1) *soit résoluble.*

A cette fin nous utilisons les points du plan. Rappelons que la représentation des nombres réels par les points d'une ligne droite (basée sur la correspondance bijective entre ces points et les nombres réels, la correspondance en question étant définie de façon suivante: on fixe l'origine et l'unité de mesure et l'on fait correspondre à tout point de la droite l'abscisse de ce point) est utilisée systématiquement par toutes les branches mathématiques et est déjà tellement familière qu'on ne fait plus de distinction entre les points d'une droite et les nombres réels représentés par ces points.

Ainsi, *nous voulons définir un ensemble de nombres représentés par les points d'un plan.* Jusqu'ici nous n'avons pas eu à additionner et à multiplier les points d'un plan, de sorte que nous sommes libres de définir ces opérations comme nous le désirons. Toutefois, en introduisant l'addition et la multiplication des points d'un plan, nous devons prendre quelques précautions afin que le système de nombres, obtenu de cette manière, jouisse de toutes les propriétés qui nous ont poussés à étendre la notion de nombre réel. Les définitions de ces opérations, surtout celle de multiplication, paraissent au début assez bizarres. On montrera dans le chapitre X qu'*aucune définition, différente de celle qu'on va donner ici*, ne pourra nous conduire à un système de nombres généralisant les nombres réels et contenant les racines de l'équation (1). On démontrera également dans ce même chapitre qu'*en remplaçant les points d'un plan par tout autre système d'êtres, on ne peut pas obtenir les nombres dont les propriétés algébriques diffèrent de celles des nombres complexes que nous allons définir dans ce paragraphe.*

Soit un plan dans lequel on se donne un système de coordonnées rectangulaires. On convient de désigner les points du plan par les lettres grecques α, β, γ,. . . et on note un point α par (a, b) si son abscisse et son ordonnée sont respectivement a et b: $\alpha = (a, b)$. Soient deux points $\alpha = (a, b)$ et $\beta = (c, d)$. La *somme* de ces points est un point dont l'abscisse est $(a + c)$ et l'ordonnée $(b + d)$, autrement dit,

$$(a, b)+(c, d)=(a+c, b+d); \tag{2}$$

le *produit* des points $\alpha=(a, b)$ et $\beta=(c, d)$ est un point ayant pour abscisse le nombre $ac-bd$ et pour ordonnée le nombre $ad+bc$, de sorte que

$$(a, b)(c, d)=(ac-bd,\ ad+bc). \quad (3$$

Ainsi, les formules (2) et (3) définissent deux opérations algébriques sur l'ensemble des points d'un plan. Montrons qu'*elles jouissent de toutes les propriétés fondamentales des opérations algébriques analogues sur l'ensemble des nombres réels (ou des nombres rationnels), à savoir que ces opérations sont commutatives, associatives, distributives*

et ont pour opérations inverses respectivement la soustraction et la division (excepté la division par zéro).

Il est clair que l'addition est commutative et associative (ce qui résulte précisément des propriétés analogues de l'addition des nombres réels), car, selon (2), on additionne séparément les abscisses et les ordonnées. Les coordonnées des points α et β intervenant symétriquement dans (3), la commutativité de la multiplication en découle immédiatement. L'associativité de la multiplication est la conséquence des égalités:

$$[(a, b)(c, d)](e, f) = (ac - bd, ad + bc)(e, f) =$$
$$= (ace - bde - adf - bcf, \ acf - bdf + ade + bce),$$
$$(a, b)[(c, d)(e, f)] = (a, b)(ce - df, cf + de) =$$
$$= (ace - adf - bcf - bde, \ acf + ade + bce - bdf).$$

Les relations

$$[(a, b) + (c, d)](e, f) = (a + c, b + d)(e, f) =$$
$$= (ae + ce - bf - df, \ af + cf + be + de),$$
$$(a, b)(e, f) + (c, d)(e, f) = (ae - bf, af + be) + (ce - df, cf + de) =$$
$$= (ae - bf + ce - df, \ af + be + cf + de)$$

établissent la loi de distributivité.

Passons aux opérations inverses. Soient deux points $\alpha = (a, b)$ et $\beta = (c, d)$. Leur différence est un point (x, y) tel que

$$(c, d) + (x, y) = (a, b),$$

d'où, en vertu de (2), les égalités:

$$c + x = a, \quad d + y = b.$$

Ainsi, la *différence* des points $\alpha = (a, b)$ et $\beta = (c, d)$ est le point

$$\alpha - \beta = (a - c, b - d) \tag{4}$$

qui est bien défini.

En particulier, l'*élément nul* dans notre système de nombres est l'origine (0, 0) et le point *opposé* à $\alpha = (a, b)$ est

$$-\alpha = (-a, -b). \tag{5}$$

Soient, maintenant, deux points $\alpha = (a, b)$ et $\beta = (c, d)$, $\beta \neq 0$. c'est-à-dire au moins l'une des coordonnées c et d n'est pas nulle, de sorte que $c^2 + d^2 \neq 0$. On appelle quotient de la division de α par β un point (x, y) tel que $(c, d)(x, y) = (a, b)$. On en déduit. en vertu de (3), les égalités:

$$cx - dy = a,$$
$$dx + cy = b.$$

En résolvant ce système d'équations, il vient :

$$x = \frac{ac+bd}{c^2+d^2}, \qquad y = \frac{bc-ad}{c^2+d^2}.$$

Ainsi, pour $\beta \neq 0$, le *quotient* $\frac{\alpha}{\beta}$ existe et est bien défini par la formule :

$$\frac{\alpha}{\beta} = \left(\frac{ac+bd}{c^2+d^2}, \ \frac{bc-ad}{c^2+d^2} \right). \tag{6}$$

Si l'on pose $\beta = \alpha$, on voit que le rôle de l'*unité* dans notre système de nombres est joué par le point (1, 0), situé sur l'axe des abscisses à la distance 1 de l'origine dans le sens positif. Posant dans (6) $\alpha = 1 = (1, 0)$, on obtient le point *inverse* du point β, $\beta \neq 0$:

$$\beta^{-1} = \left(\frac{c}{c^2+d^2}, \ \frac{-d}{c^2+d^2} \right). \tag{7}$$

Ainsi, nous avons construit un système de nombres représentés par les points d'un plan ; en outre, les formules (2) et (3) définissent deux opérations algébriques, l'addition et la multiplication, sur l'ensemble de ces nombres. Cet ensemble est appelé *système de nombres complexes.*

Montrons que *les nombres réels constituent un cas particulier des nombres complexes.* Considérons pour cela les points situés sur l'axe des abscisses, c'est-à-dire les points de la forme $(a, 0)$; faisant correspondre au point $(a, 0)$ le nombre réel a, nous obtenons, bien entendu, une correspondance bijective entre l'ensemble des points de l'axe des abscisses et celui des nombres réels. L'application des formules (2) et (3) à ces points donne les égalités

$$(a, 0) + (b, 0) = (a+b, 0),$$
$$(a, 0) \cdot (b, 0) = (ab, 0) ;$$

autrement dit, les règles d'addition et de multiplication des points de l'axe des abscisses sont exactement les mêmes que celles d'addition et de multiplication des nombres réels correspondants. Ainsi, *l'ensemble des points appartenant à l'axe des abscisses, considéré comme un sous-ensemble de l'ensemble des nombres complexes, jouit exactement des mêmes propriétés algébriques que celui des nombres réels représentés, comme d'habitude, par les points d'une ligne droite.* Ceci nous autorise à ne pas faire de distinction entre le point $(a, 0)$ et le nombre réel a, posant chaque fois $(a, 0) = a$. En particulier, l'élément nul (0, 0) et l'élément unité (1, 0) du système de nombres complexes sont respectivement les nombres réels 0 et 1.

Il nous faut montrer à présent que *l'équation* (1) *est résoluble dans l'ensemble des nombres complexes*, c'est-à-dire il faut prouver l'existence d'un nombre complexe tel que ce nombre élevé à la

puissance deux donne le nombre réel — 1. Le point (0, 1) possède, par exemple, cette propriété. (Rappelons que (0, 1) est le point situé sur l'axe des ordonnées à la distance 1 de l'origine dans le sens positif.) En effet, appliquant (3), il vient:

$$(0, 1)\cdot(0, 1) = (-1, 0) = -1.$$

Convenons de noter ce point par le symbole i, de sorte que $i^2 = -1$.

Montrons enfin que *les nombres complexes introduits ci-dessus peuvent être représentés sous la forme habituelle.* Pour cela, trouvons d'abord le produit du nombre réel b par le point i:

$$bi = (b, 0)\cdot(0, 1) = (0, b);$$

ainsi, bi est un point situé sur l'axe des ordonnées, d'ordonnée b; en outre, tout point de l'axe des ordonnées peut être représenté sous la forme du produit d'un nombre réel par i. Soit, à présent, (a, b) un point quelconque; alors, en vertu de l'égalité

$$(a, b) = (a, 0) + (0, b),$$

il vient:

$$(a, b) = a + bi,$$

c'est-à-dire nous retrouvons la forme habituelle des nombres complexes; évidemment, dans cette représentation on entend par addition et multiplication les opérations définies par les formules (2) et (3) sur l'ensemble des nombres complexes.

Maintenant que les nombres complexes sont définis, le lecteur voudra bien nous croire que le *contenu des chapitres précédents,* notamment la théorie des déterminants et celle des systèmes d'équations linéaires, ainsi que les résultats se rapportant aux vecteurs et aux matrices, est *valable sans restriction aucune lorsqu'on se place dans le cas des nombres complexes.*

Faisons encore quelques remarques pour terminer le paragraphe. L'introduction du système de nombres complexes à l'aide de la représentation par les points d'un plan suscite un autre problème: peut-on définir l'addition et la multiplication des points de l'espace à trois dimensions de telle manière que le système de nombres, obtenu par ce procédé, contienne les nombres complexes ou, du moins, les nombres réels? L'étude de ce problème sort du cadre de notre cours et nous nous bornerons à dire que la réponse à la question posée est négative.

D'autre part, observant que l'addition des nombres complexes est équivalente à celle des vecteurs issus de l'origine dans un plan (cf. le paragraphe suivant), il est naturel de poser la question suivante: peut-on définir dans l'espace vectoriel réel à n dimensions, ne serait-ce que pour certaines valeurs de l'entier n, une multiplication de vecteurs de telle façon que, muni de cette multiplication

et de l'addition habituelle, l'espace vectoriel réel devienne un système de nombres, contenant le sous-système de nombres réels? On peut montrer que cela est impossible si l'on veut conserver toutes les propriétés de ces opérations algébriques qui ont lieu dans le cas des nombres rationnels, réels et complexes. Mais, renonçant à la commutativité de la multiplication, une telle construction devient possible pour $n = 4$; le système de nombres correspondants est dit le *système des quaternions.* La même chose peut être faite dans l'espace à 8 dimensions, le système correspondant est appelé *système des nombres de Cayley.* Dans ce dernier cas on est obligé de renoncer non seulement à la commutativité, mais aussi à l'associativité de la multiplication, en remplaçant cette dernière par une condition plus faible.

§ 18. Suite de l'étude des nombres complexes

Selon la tradition, nous continuerons à appeler *unité imaginaire* le nombre complexe i; les nombres bi sont dits *imaginaires*, quoique leur existence ne suscite aucun doute et l'on peut indiquer les points du plan (ce sont ceux de l'axe des ordonnées) qui correspondent à ces nombres. Si le nombre complexe α est représenté sous la forme: $\alpha = a + bi$, alors a et bi sont dits respectivement la *partie réelle* et la *partie imaginaire* de α. On appelle *plan complexe* le plan dont les points s'identifient aux nombres complexes conformément à la règle exposée au § 17. L'axe des abscisses est dit *réel*, ses points correspondant aux nombres réels, de même l'axe des ordonnées est dit *imaginaire.*

Les formules (2), (4), (3) et (6) du paragraphe précédent, appliquées aux nombres complexes représentés sous la forme $a + bi$, donnent les relations:

$$(a+bi)+(c+di)=(a+c)+(b+d)\,i;$$
$$(a+bi)-(c+di)=(a-c)+(b-d)\,i;$$
$$(a+bi)(c+di)=(ac-bd)+(ad+bc)\,i;$$
$$\frac{a+bi}{c+di}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}\,i.$$

Autrement dit, il faut, *pour trouver la somme de nombres complexes, additionner séparément leurs parties réelles et leurs parties imaginaires*; la règle analogue est valable pour la soustraction. On ne donne pas ici d'énoncé de la règle de multiplication et de division des nombres complexes, cet énoncé étant trop long. On n'a pas besoin de garder dans la mémoire la dernière formule. Il suffit de retenir le procédé permettant de l'établir. Pour cela il faut multiplier le numérateur et le dénominateur par le nombre complexe $c - di$.

En effet, on a

$$\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)\,i}{c^2+d^2}=$$
$$=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}\,i.$$

Exemples.

1) $(2+5i)+(1-7i)=(2+1)+(5-7)\,i=3-2i$;

2) $(3-9i)-(7+i)=(3-7)+(-9-1)\,i=-4-10i$;

3) $(1+2i)(3-i)=[1\cdot3-2\cdot(-1)]+[1\cdot(-1)+2\cdot3]\,i=5+5i$;

4) $\dfrac{23+i}{3+i}=\dfrac{(23+i)(3-i)}{(3+i)(3-i)}=\dfrac{70-20i}{10}=7-2i.$

La représentation des nombres complexes par les points du plan pose naturellement le problème d'interpréter géométriquement les opérations algébriques définies dans l'ensemble des nombres complexes. Il n'est pas du tout difficile de donner l'interprétation géométrique de l'addition. En effet, soient deux nombres $\alpha = a + bi$

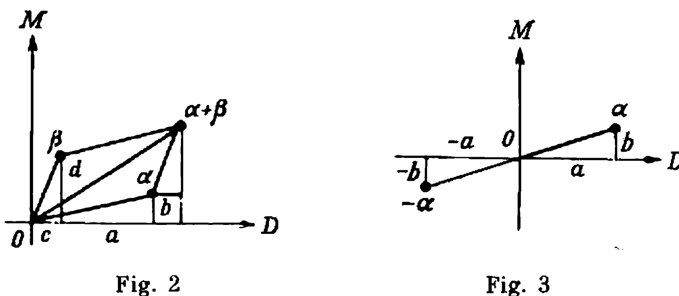


Fig. 2 Fig. 3

et $\beta = c + di$. Alors, le quatrième sommet du parallélogramme dont les trois autres sommets sont respectivement α, 0 et β représente la somme $\alpha + \beta = (a + c,\ b + d)$ (fig. 2). Ainsi, *l'addition des nombres complexes est en réalité celle des vecteurs issus de l'origine.* Ensuite, *le nombre opposé au nombre $\alpha = a + bi$ est représenté par le point symétrique du point α par rapport à l'origine* (fig. 3). On en déduit facilement l'interprétation géométrique de la soustraction.

Le sens géométrique de la multiplication et de la division des nombres complexes ne sera clair que lorsque nous aurons introduit une autre écriture des nombres complexes. On utilise pour représenter un nombre complexe α sous la forme $\alpha = a + bi$ les coordonnées cartésiennes du point correspondant. Or, un point du plan est également bien déterminé par ses coordonnées polaires, c'est-à-dire par la distance r du point α à l'origine et par l'angle φ que le rayon vecteur de α forme avec le sens positif de l'axe des abscisses (fig. 4).

Le nombre r est réel et non négatif ; en outre, $r = 0$ seulement pour le point 0. Si α appartient à l'axe réel, c'est-à-dire si le nombre α est réel, alors r est la *valeur absolue* de α, de sorte qu'on emploie quelquefois ce terme même lorsque α est complexe ; plus souvent, on appelle r *module* du nombre α et on le note par $|\alpha|$.

L'angle φ est dit *argument* du nombre α et est noté par le symbole $\arg \alpha$ [1]. Le nombre φ est un nombre réel quelconque, les valeurs négatives et positives de φ correspondant respectivement aux angles comptés dans le sens des aiguilles d'une montre et dans le sens opposé. En outre, si la distance r est constante, les valeurs de φ différant de $2\pi q$, où q est un entier, définissent le même point du plan.

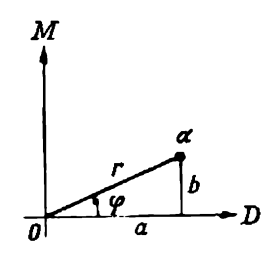


Fig. 4

Ainsi, l'argument du nombre complexe α peut prendre une infinité de valeurs, dont la différence est toujours égale à $2\pi q$, où q est un entier. Ainsi, deux nombres complexes, donnés par leurs modules et arguments, ne sont égaux que lorsque les modules coïncident et les arguments diffèrent d'un multiple de 2π. L'argument du nombre 0 n'est pas défini ; n'empêche que ce nombre est bien déterminé par l'égalité : $|0| = 0$.

L'argument d'un nombre complexe est la généralisation naturelle du signe d'un nombre réel. En effet, l'argument d'un nombre réel positif est zéro et celui d'un nombre réel négatif est π ; dans le cas de l'axe réel il n'y a que deux demi-droites issues de l'origine des coordonnées et l'on peut les affecter de deux signes + et —, tandis que dans le cas du plan complexe il existe une infinité de demi-droites issues du point 0 et il est logique, pour les discerner, de faire correspondre à chaque demi-droite l'angle formé par elle et par la demi-droite des x positifs de l'axe réel.

La relation entre les coordonnées polaires et cartésiennes est donnée par les égalités suivantes :

$$a = r\cos\varphi, \quad b = r\sin\varphi, \tag{1}$$

d'où

$$r = +\sqrt{a^2 + b^2}. \tag{2}$$

Les formules (1) appliquées à un nombre complexe $\alpha = a + bi$ donnent

$$\alpha = a + bi = r\cos\varphi + (r\sin\varphi)\,i$$

[1] Nous renonçons donc aux termes traditionnels, rayon et angle, pour désigner les coordonnées polaires d'un point du plan.

ou encore

$$\alpha = r(\cos\varphi + i\sin\varphi). \qquad (3)$$

Réciproquement, soit $\alpha = a + bi = r_0(\cos\varphi_0 + i\sin\varphi_0)$, où r_0 est non négatif, φ_0 réel. Alors $r_0\cos\varphi_0 = a$, $r_0\sin\varphi_0 = b$, de sorte qu'en vertu de (2), $r_0 = +\sqrt{a^2+b^2} = |\alpha|$. On en déduit, en utilisant (1), que $\cos\varphi = \cos\varphi_0$, $\sin\varphi = \sin\varphi_0$, c'est-à-dire que $\varphi_0 = \arg\alpha$. Ainsi, *tout nombre complexe* α *peut être représenté de façon unique sous la forme* (3) *avec* $r = |\alpha|$ et $\varphi = \arg\alpha$ (évidemment, $\arg\alpha$ est défini à $2\pi q$ près, q étant un entier). Cette représentation est appelée *forme trigonométrique* du nombre complexe α. Elle sera beaucoup utilisée dans tout ce qui suit.

Les nombres

$$\alpha = 3\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right), \qquad \beta = \cos\frac{19}{3}\pi + i\sin\frac{19}{3}\pi,$$

$$\gamma = \sqrt{3}\left[\cos\left(-\frac{\pi}{7}\right) + i\sin\left(-\frac{\pi}{7}\right)\right]$$

sont donnés sous la forme trigonométrique ; ici $|\alpha| = 3$, $|\beta| = 1$, $|\gamma| = \sqrt{3}$; $\arg\alpha = \frac{\pi}{4}$, $\arg\beta = \frac{19}{3}\pi$, $\arg\gamma = -\frac{\pi}{7}$ $\left(\text{ou bien } \arg\beta = \frac{\pi}{3},\ \arg\gamma = \frac{13}{7}\pi\right)$

D'autre part, les nombres complexes

$$\alpha' = (-2)\left(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right), \quad \beta' = 3\left(\cos\frac{2}{3}\pi - i\sin\frac{2}{3}\pi\right),$$

$$\gamma' = 2\left(\cos\frac{\pi}{3} + i\sin\frac{3}{4}\pi\right), \quad \delta' = \sin\frac{3}{4}\pi + i\cos\frac{3}{4}\pi$$

ne sont pas donnés sous la forme trigonométrique, cette dernière s'écrivant pour ces nombres de la manière suivante :

$$\alpha' = 2\left(\cos\frac{6}{5}\pi + i\sin\frac{6}{5}\pi\right), \qquad \beta' = 3\left(\cos\frac{4}{3}\pi + i\sin\frac{4}{3}\pi\right),$$

$$\delta' = \cos\frac{7}{4}\pi + i\sin\frac{7}{4}\pi.$$

Essayant de trouver la forme trigonométrique de γ' nous nous heurtons à une difficulté qui est propre au passage de la forme cartésienne des nombres complexes à la forme trigonométrique : nous ne pouvons pas toujours trouver la valeur exacte de l'angle dont nous connaissons les sinus et cosinus ; l'inverse a également lieu : nous ne sommes pas toujours capables de déterminer les valeurs numériques *exactes* des fonctions trigonométriques d'un angle donné.

Soient deux nombres complexes α et β représentés sous la forme trigonométrique : $\alpha = r(\cos\varphi + i\sin\varphi)$, $\beta = r'(\cos\varphi' + i\sin\varphi')$. Calculons leur produit :

$$\alpha\beta = [r(\cos\varphi + i\sin\varphi)]\cdot[r'(\cos\varphi' + i\sin\varphi')] =$$
$$= rr'(\cos\varphi\cos\varphi' + i\cos\varphi\sin\varphi' + i\sin\varphi\cos\varphi' - \sin\varphi\sin\varphi'),$$

ou encore

$$\alpha\beta = rr' [\cos(\varphi + \varphi') + i \sin(\varphi + \varphi')]. \qquad (4)$$

Nous avons obtenu le produit sous la forme trigonométrique, de sorte que $|\alpha\beta| = rr'$, ou encore

$$|\alpha\beta| = |\alpha| \, |\beta|; \qquad (5)$$

autrement dit, le *module du produit de nombres complexes est égal au produit des modules des facteurs*. Ensuite, $\arg(\alpha\beta) = \varphi + \varphi'$, ou encore

$$\arg(\alpha\beta) = \arg\alpha + \arg\beta; \qquad (6)$$

en d'autres termes, l'*argument du produit de nombres complexes est égal à la somme des arguments des facteurs* [1]. Bien entendu, ces règles s'étendent à un nombre quelconque fini de facteurs. Dans le cas des nombres réels la formule (5) représente la propriété bien connue des valeurs absolues, tandis que la relation (6) donne la règle des signes de la multiplication.

La formule analogue a lieu pour le quotient. En effet, soient $\alpha = r(\cos\varphi + i \sin\varphi)$, $\beta = r'(\cos\varphi' + i \sin\varphi')$, $\beta \neq 0$, c'est-à-dire $r' \neq 0$. Alors

$$\frac{\alpha}{\beta} = \frac{r(\cos\varphi + i \sin\varphi)}{r'(\cos\varphi' + i \sin\varphi')} = \frac{r(\cos\varphi + i \sin\varphi)(\cos\varphi' - i \sin\varphi')}{r'(\cos^2\varphi' + \sin^2\varphi')} =$$

$$= \frac{r}{r'}(\cos\varphi\cos\varphi' + i \sin\varphi\cos\varphi' - i \cos\varphi\sin\varphi' + \sin\varphi\sin\varphi'),$$

ou encore

$$\frac{\alpha}{\beta} = \frac{r}{r'}[\cos(\varphi - \varphi') + i \sin(\varphi - \varphi')]. \qquad (7)$$

D'où il vient $\left|\frac{\alpha}{\beta}\right| = \frac{r}{r'}$ ou encore

$$\left|\frac{\alpha}{\beta}\right| = \frac{|\alpha|}{|\beta|}, \qquad (8)$$

c'est-à-dire que le *module du quotient de deux nombres complexes est le quotient des modules de ces nombres*; puis $\arg\left(\frac{\alpha}{\beta}\right) = \varphi - \varphi'$ ou encore

$$\arg\left(\frac{\alpha}{\beta}\right) = \arg\alpha - \arg\beta, \qquad (9)$$

autrement dit, l'*argument du quotient de deux nombres complexes s'obtient en retranchant de l'argument du numérateur l'argument du dénominateur.*

[1] Il est sous-entendu que cette égalité a lieu à un multiple de 2π près.

Maintenant nous sommes en mesure de donner l'interprétation géométrique de la multiplication et de la division. En effet, en vertu des formules (5) et (6), le point représentant le produit des nombres α et $\beta = r' (\cos \varphi' + i \sin \varphi')$ est le résultat des transformations géométriques suivantes: rotation du rayon vecteur du nombre

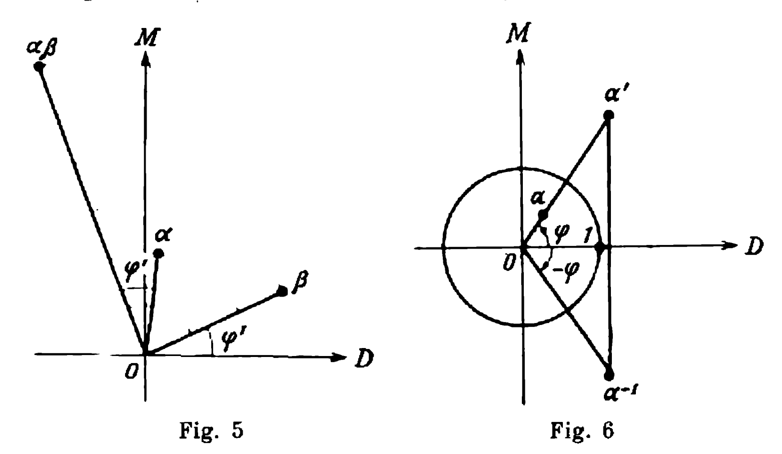


Fig. 5 Fig. 6

complexe α (fig. 5), d'angle $\varphi' = \arg \beta$, dans le sens contraire à celui des aiguilles d'une montre et extension de la longueur du vecteur de $r' = |\beta|$ fois (contraction, pour $0 \leqslant r' < 1$). Ensuite, si $\alpha = r (\cos \varphi + i \sin \varphi) \neq 0$, la formule (7) donne

$$\alpha^{-1} = r^{-1} [\cos(-\varphi) + i \sin(-\varphi)], \tag{10}$$

c'est-à-dire $\arg(\alpha^{-1}) = -\arg \alpha$ et $|\alpha^{-1}| = |\alpha|^{-1}$. Ainsi, on obtient le point α^{-1}, en passant du point α au point α' qui se trouve à la distance r^{-1} de l'origine sur la même demi-droite issue de 0 que α (fig. 6)[1] après quoi il faut prendre le point symétrique de α' par rapport à l'axe réel.

On ne peut pas donner de formules analogues aux formules (4) et (7) pour la somme et la différence de deux nombres complexes écrits sous la forme trigonométrique. Toutefois, on a les inégalités très importantes:

$$|\alpha| - |\beta| \leqslant |\alpha + \beta| \leqslant |\alpha| + |\beta|, \tag{11}$$

c'est-à-dire le *module de la somme de deux nombres complexes est inférieur ou égal à la somme de leurs modules, et il est supérieur ou*

[1] Il faut noter que $|\alpha'| = |\alpha|$ si et seulement si $|\alpha| = 1$, c'est-à-dire si le point α appartient à la circonférence de rayon 1. Si α se trouve à l'intérieur du cercle de rayon 1, alors α' est situé à l'extérieur de ce cercle et inversement. Faisant correspondre au point α, $\alpha \neq 0$, le point α', nous obtenons une application bijective du cercle de rayon 1 sur la partie extérieure à ce cercle.

égal à la différence de ces modules. On établit les inégalités (11) à l'aide d'un théorème de la géométrie élémentaire sur les côtés d'un triangle. On laisse au lecteur le soin de voir le cas particulier où α, β et 0 se trouvent sur une droite ; ce n'est que dans ce cas que l'une ou l'autre des relations (11) se transforme en une égalité.

Etant donné que $\alpha-\beta=\alpha+(-\beta)$ et

$$|-\beta|=|\beta| \tag{12}$$

(cette relation résulte ne serait-ce que de l'interprétation géométrique du nombre $-\beta$), on déduit de (11) :

$$|\alpha|-|\beta|\leqslant|\alpha-\beta|\leqslant|\alpha|+|\beta|, \tag{13}$$

c'est-à-dire les mêmes inégalités pour $|\alpha-\beta|$ que pour $|\alpha+\beta|$.

On aurait pu établir les inégalités (11) de la façon suivante. Soient $\alpha = r(\cos\varphi + i\sin\varphi)$, $\beta = r'(\cos\varphi' + i\sin\varphi')$ et soit $\alpha+\beta = R(\cos\psi + i\sin\psi)$ la forme trigonométrique du nombre complexe $\alpha+\beta$. Ajoutant séparément les parties réelles et imaginaires, il vient :

$$r\cos\varphi + r'\cos\varphi' = R\cos\psi,$$
$$r\sin\varphi + r'\sin\varphi' = R\sin\psi;$$

en multipliant les deux membres de ces égalités respectivement par $\cos\psi$ et par $\sin\psi$ et en les ajoutant, nous obtenons :

$$r(\cos\varphi\cos\psi+\sin\varphi\sin\psi)+r'(\cos\varphi'\cos\psi+\sin\varphi'\sin\psi)=$$
$$=R(\cos^2\psi+\sin^2\psi),$$

c'est-à-dire

$$r\cos(\varphi-\psi)+r'\cos(\varphi'-\psi)=R.$$

Le cosinus d'un angle étant, en valeur absolue, inférieur ou égal à un, il en résulte l'inégalité : $r + r' \geqslant R$ ou encore $|\alpha| + |\beta| \geqslant |\alpha+\beta|$. D'autre part, on a $\alpha = (\alpha+\beta) - \beta = (\alpha+\beta) + (-\beta)$. Il en découle, selon l'inégalité que nous venons de démontrer et compte tenu de (12), que

$$|\alpha|\leqslant|\alpha+\beta|+|-\beta|=|\alpha+\beta|+|\beta|,$$

d'où l'on a $|\alpha|-|\beta|\leqslant|\alpha+\beta|$.

Il faut remarquer que l'ensemble des nombres complexes n'est pas ordonné, ces nombres étant représentés par les points d'un plan, de sorte qu'un nombre complexe ne peut pas être supérieur ou inférieur à un autre nombre complexe, ce qui n'est pas le cas de l'ensemble des nombres réels identifiés aux points de l'axe réel et, pour cette raison, ordonnés de façon naturelle. C'est pourquoi *on peut établir des inégalités pour les modules et non pas pour les nombres complexes eux-mêmes.*

Nombres complexes conjugués. Soit un nombre complexe $\alpha = a + bi$. Le nombre $a - bi$, noté $\bar{\alpha}$, est dit *conjugué* du nombre α.

Rappelons que nous avons déjà utilisé les nombres complexes pour la division bien que nous n'ayons pas employé ce terme.

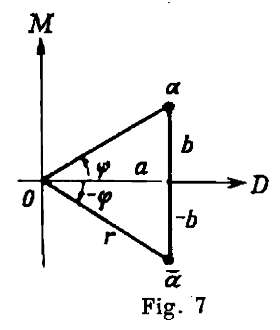


Fig. 7

Evidemment le conjugué de $\bar{\alpha}$ est encore α, de sorte qu'on peut parler d'un couple de nombres complexes conjugués. Tout nombre réel coïncide avec son conjugué; la réciproque est également vraie: si un nombre complexe coïncide avec son conjugué, c'est qu'il est réel.

L'interprétation géométrique d'un couple de nombres conjugués est la suivante: ces nombres sont des points symétriques par rapport à l'axe réel (fig. 7). On en déduit les égalités:

$$|\bar{\alpha}| = |\alpha|, \quad \arg \bar{\alpha} = -\arg \alpha. \tag{14}$$

La somme et le produit des nombres complexes conjugués sont des nombres réels. En effet,

$$\left.\begin{aligned} \alpha + \bar{\alpha} &= 2a, \\ \alpha\bar{\alpha} &= a^2 + b^2 = |\alpha|^2. \end{aligned}\right\} \tag{15}$$

La dernière égalité montre que $\alpha\bar{\alpha}$ est positif si $\alpha \neq 0$. On montrera au § 24 que cette propriété des couples de nombres complexes conjugués leur est caractéristique.

L'identité

$$(a - bi) + (c - di) = (a + c) - (b + d)\,i$$

montre que le *nombre complexe conjugué de la somme de deux nombres complexes est la somme des nombres conjugués de chaque terme de la somme*:

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}. \tag{16}$$

De même, l'identité

$$(a - bi)(c - di) = (ac - bd) - (ad + bc)\,i$$

montre que le *nombre complexe conjugué du produit est égal au produit des nombres conjugués de chaque facteur*:

$$\overline{\alpha\beta} = \bar{\alpha} \cdot \bar{\beta}. \tag{17}$$

La vérification directe donne les formules

$$\overline{\alpha-\beta}=\bar{\alpha}-\bar{\beta}, \tag{18}$$

$$\overline{\left(\frac{\alpha}{\beta}\right)}=\frac{\bar{\alpha}}{\bar{\beta}}. \tag{19}$$

Démontrons la proposition suivante: si le nombre complexe α s'exprime par les nombres complexes $\beta_1, \beta_2, \ldots, \beta_n$ au moyen des quatre opérations algébriques (addition, soustraction, multiplication et division), alors, remplaçant dans l'expression de α les nombres $\beta_1, \ldots, \beta_k$ par leurs conjugués $\bar{\beta}_1, \ldots, \bar{\beta}_k$, on obtient $\bar{\alpha}$. En particulier, si α est réel, en remplaçant β_k par $\bar{\beta}_k$ on ne modifie pas la valeur de α.

Démontrons cette proposition par récurrence sur n, étant donné que pour $n=2$ elle est évidente en vertu des formules (16)-(19).

Supposons que le nombre α s'exprime par les nombres $\beta_1, \beta_2, \ldots$ $\ldots, \beta_n$ (pas forcément tous distincts). Dans cette expression les opérations algébriques sont appliquées dans un ordre déterminé. L'opération finale est appliquée à un nombre γ_1, exprimé par β_1, $\beta_2, \ldots, \beta_k$, $1 \leqslant k \leqslant n-1$, et à un nombre γ_2, exprimé par $\beta_{k+1}, \ldots, \beta_n$. En vertu de l'hypothèse de récurrence, γ_1 est remplacé par $\bar{\gamma}_1$ quand on remplace $\beta_1, \ldots, \beta_k$ par $\bar{\beta}_1, \ldots, \bar{\beta}_k$, de même que γ_2 est remplacé par $\bar{\gamma}_2$ si l'on remplace $\beta_{k+1}, \ldots, \beta_n$ par $\bar{\beta}_{k+1}, \ldots, \bar{\beta}_n$. Or, les formules (16)-(19) montrent que le passage des nombres γ_1 et γ_2 aux nombres $\bar{\gamma}_1$ et $\bar{\gamma}_2$ remplace le nombre α par le nombre $\bar{\alpha}$.

§ 19. Extraction de racine des nombres complexes

Nous nous occuperons dans ce paragraphe des puissances et des racines des nombres complexes. Pour élever un nombre complexe $\alpha = a + bi$ à la puissance $n^{\text{ème}}$ (n est un entier positif), il suffit d'appliquer à l'expression $(a+bi)^n$ la formule du binôme de Newton (cette formule est valable pour les nombres complexes, car sa démonstration n'est basée que sur la loi de distributivité) en tenant compte des égalités: $i^2=-1$, $i^3=-i$, $i^4=1$ et, plus généralement, des égalités

$$i^{4k}=1,\ i^{4k+1}=i,\ i^{4k+2}=-1,\ i^{4k+3}=-i.$$

Le nombre complexe α étant représenté sous la forme trigonométrique, la relation (4) du paragraphe précédent donne immédiatement l'égalité, dite *formule de Moivre*:

$$[r(\cos\varphi+i\sin\varphi)]^n=r^n(\cos n\varphi+i\sin n\varphi), \tag{1}$$

où n est un entier positif quelconque. Ainsi, *pour élever un nombre complexe à la puissance $n^{\text{ème}}$, il faut élever à la puissance $n^{\text{ème}}$ son module et multiplier par n son argument.* La formule (1) est également valable pour n entier négatif. Effectivement, en vertu de l'identité $\alpha^{-n} = (\alpha^{-1})^n$, il suffit d'appliquer la formule de Moivre au nombre α^{-1} dont la forme trigonométrique est donnée par la relation (10) du paragraphe précédent.

Exemples.

1) $i^{37} = i,\ i^{122} = -1$;

2) $(2+5i)^3 = 2^3 + 3\cdot 2^2\cdot 5i + 3\cdot 2\cdot 5^2 i^2 + 5^3 i^3 =$

$$= 8 + 60i - 150 - 125i = -142 - 65i \ ;$$

3) $\left[\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)\right]^4 = (\sqrt{2})^4(\cos\pi + i\sin\pi) = -4$;

4) $\left[3\left(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right)\right]^{-3} = 3^{-3}\left[\cos\left(-\frac{3}{5}\pi\right) + \right.$

$$\left. + i\sin\left(-\frac{3}{5}\pi\right)\right] = \frac{1}{27}\left(\cos\frac{7}{5}\pi + i\sin\frac{7}{5}\pi\right)$$

Un cas particulier de la formule de Moivre, à savoir

$$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi,$$

permet d'obtenir les expressions de $\sin n\varphi$ et de $\cos n\varphi$ en fonction des puissances de $\sin\varphi$ et de $\cos\varphi$. En effet, développant le premier membre de cette égalité et séparant les parties réelle et imaginaire, il vient :

$$\cos n\varphi = \cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\cdot\sin^2\varphi + $$
$$+ \binom{n}{4}\cos^{n-4}\varphi\cdot\sin^4\varphi - \ldots ,$$
$$\sin n\varphi = \binom{n}{1}\cos^{n-1}\varphi\cdot\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\cdot\sin^3\varphi + $$
$$+ \binom{n}{5}\cos^{n-5}\varphi\cdot\sin^5\varphi - \ldots ;$$

ici $\binom{n}{k}$ est la notation habituelle du coefficient binomial :

$$\binom{n}{k} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{1\cdot 2\cdot 3\ldots k}.$$

Si $n = 2$, on retrouve les formules bien connues

$$\cos 2\varphi = \cos^2\varphi - \sin^2\varphi,$$
$$\sin 2\varphi = 2\cos\varphi\sin\varphi ;$$

si $n=3$, on obtient les relations

$$\cos 3\varphi = \cos^3\varphi - 3\cos\varphi\sin^2\varphi,$$
$$\sin 3\varphi = 3\cos^2\varphi\sin\varphi - \sin^3\varphi.$$

L'extraction de racine des nombres complexes comporte beaucoup plus de difficultés. Commençons par extraire la racine carrée d'un nombre complexe $\alpha = a + bi$. Pour le moment, nous ignorons l'existence d'un nombre complexe dont le carré serait égal à α. Supposons qu'un tel nombre existe, soit $u + vi$; alors

$$\sqrt{a+bi} = u + vi,$$

ou encore

$$a + bi = (u + vi)^2,$$

d'où il suit

$$\left.\begin{aligned} u^2 - v^2 &= a, \\ 2uv &= b. \end{aligned}\right\} \qquad (2)$$

Elevant au carré les deux membres des équations (2) et les additionnant, il vient :

$$(u^2 - v^2)^2 + 4u^2v^2 = (u^2 + v^2)^2 = a^2 + b^2,$$

d'où l'égalité

$$u^2 + v^2 = +\sqrt{a^2 + b^2};$$

le second membre de la dernière relation est affecté du signe $+$ car les nombres u et v sont réels. Cette égalité avec la première des équations (2) donne :

$$u^2 = \frac{1}{2}\left(a + \sqrt{a^2 + b^2}\right),$$
$$v^2 = \frac{1}{2}\left(-a + \sqrt{a^2 + b^2}\right).$$

Extrayant les racines carrées au sens arithmétique des seconds membres nous sommes conduits à deux valeurs opposées de u et de v. Toutes ces valeurs sont réelles, car les seconds membres dans les expressions de u^2 et v^2 sont positifs, quels que soient les nombres réels a et b. Etant donné que le signe du produit uv doit être celui du nombre b (voir la seconde des équations (2)), nous obtenons deux nombres complexes différents (et non pas quatre), représentés sous la forme $u + vi$, qui sont les racines carrées de α ; ces nombres sont opposés. Il est facile, quoiqu'un peu laborieux, de vérifier que les nombres complexes trouvés sont effectivement les racines carrées de α. Ainsi, l'*extraction de la racine carrée d'un nombre complexe quelconque est toujours possible et donne deux racines opposées.*

En particulier, nous sommes maintenant en mesure d'extraire la racine carrée d'un nombre réel négatif, dont les valeurs seront

purement imaginaires. En effet, si $a < 0$ et $b = 0$, alors $\sqrt{a^2+b^2} = -a$ (la racine carrée devant être positive), d'où il vient: $u^2 = \frac{1}{2}(a - a) = 0$, à savoir $u = 0$, de sorte que $\sqrt{a} = \pm vi$.

Exemple. Soit $\alpha = 21 - 20i$. Alors $\sqrt{a^2+b^2} = \sqrt{441+400} = 29$, de sorte que $u^2 = \frac{1}{2}(21 + 29) = 25$, $v^2 = \frac{1}{2}(-21 + 29) = 4$, ou encore $u = \pm 5$, $v = \pm 2$. Le nombre b étant négatif, les signes de u et v doivent être opposés, de sorte que

$$\sqrt{21-20i} = \pm(5-2i).$$

Si on essaye d'extraire d'un nombre complexe de la forme $a + bi$ une racine d'ordre supérieur à deux, on se heurte à des difficultés insurmontables. Ainsi, comme on le verra au § 38, si nous voulons extraire la racine cubique d'un nombre complexe $a + bi$, il est nécessaire de résoudre une équation auxiliaire du troisième degré, ce qui exige, à son tour, l'extraction de la racine cubique d'un nombre complexe. D'autre part, la forme trigonométrique s'y prête parfaitement et permet de résoudre complètement ce problème.

Soit un nombre complexe $\alpha = r(\cos\varphi + i\sin\varphi)$ dont il faut extraire la racine $n^{\text{ème}}$. Supposons que cela soit possible et que $\rho(\cos\theta + i\sin\theta)$ soit la racine en question, de sorte que nous avons l'identité

$$[\rho(\cos\theta + i\sin\theta)]^n = r(\cos\varphi + i\sin\varphi). \tag{3}$$

La formule de Moivre donne $\rho^n = r$, ou encore $\rho = \sqrt[n]{r}$; ici $\sqrt[n]{r}$ est la valeur positive bien définie de la racine $n^{\text{ème}}$ d'un nombre réel positif (au sens arithmétique). D'autre part, l'argument du premier membre dans (3) est égal à $n\theta$. Néanmoins, on ne peut pas dire que $n\theta$ soit égal à φ, mais, de toute façon, on a $n\theta = \varphi + 2\pi k$, où k est un entier, d'où il vient

$$\theta = \frac{\varphi + 2\pi k}{n}.$$

Réciproquement, le nombre $\sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right)$, *quel que soit l'entier k, positif ou négatif*, élevé à la puissance $n^{\text{ème}}$, est égal au nombre α. Ainsi,

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right). \tag{4}$$

Le paramètre k parcourant l'ensemble des nombres entiers, il arrive parfois que certaines racines $n^{\text{èmes}}$, correspondant aux différents k, coïncident. En effet, si k prend respectivement les valeurs:

$$k = 0,\ 1,\ 2, \ldots,\ n-1, \tag{5}$$

alors nous obtenons n racines $n^{\text{èmes}}$ distinctes de α, car remplaçant k par $k+1$, l'argument de la racine augmente de $\frac{2\pi}{n}$. Soit, à présent, k un entier quelconque et $k = nq + r$, avec r et q entiers, $0 \leqslant r \leqslant n-1$. Alors

$$\frac{\varphi + 2\pi k}{n} = \frac{\varphi + 2(nq + r)\pi}{n} = \frac{\varphi + 2\pi r}{n} + 2\pi q,$$

de sorte que nous avons la même racine $n^{\text{ème}}$ que pour $k = r$, car les arguments correspondants se distinguent l'un de l'autre de $2\pi q$.

Ainsi, *il est toujours possible d'extraire la racine $n^{\text{ème}}$ d'un nombre complexe, celle-ci ayant n valeurs distinctes. Les racines $n^{\text{èmes}}$ d'un nombre α se trouvent toutes sur la circonférence de rayon $\sqrt[n]{|\alpha|}$ et de centre* 0, *la distance entre deux valeurs voisines étant constante.*

En particulier, la racine $n^{\text{ème}}$ d'un nombre réel a a n valeurs distinctes ; selon le signe de a et de la parité de n il y a tout au plus deux valeurs réelles parmi ces racines.

Exemples.

1) $$\beta = \sqrt[3]{2\left(\cos\frac{3}{4}\pi + i\sin\frac{3}{4}\pi\right)} = \sqrt[3]{2}\left(\cos\frac{\frac{3}{4}\pi + 2\pi k}{3} + i\sin\frac{\frac{3}{4}\pi + 2\pi k}{3}\right);$$

$$k=0: \ \beta_0 = \sqrt[3]{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right);$$

$$k=1: \ \beta_1 = \sqrt[3]{2}\left(\cos\frac{11}{12}\pi + i\sin\frac{11}{12}\pi\right);$$

$$k=2: \ \beta_2 = \sqrt[3]{2}\left(\cos\frac{19}{12}\pi + i\sin\frac{19}{12}\pi\right).$$

2) $$\beta = \sqrt{i} = \sqrt{\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}} = \cos\frac{\frac{\pi}{2} + 2\pi k}{2} + i\sin\frac{\frac{\pi}{2} + 2\pi k}{2};$$

$$\beta_0 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2};$$

$$\beta_1 = \cos\frac{5}{4}\pi + i\sin\frac{5}{4}\pi = -\beta_0.$$

3) $$\beta = \sqrt[3]{-8} = \sqrt[3]{8(\cos\pi + i\sin\pi)} = 2\left(\cos\frac{\pi + 2\pi k}{3} + i\sin\frac{\pi + 2\pi k}{3}\right);$$

$$\beta_0 = 2\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) = 1 + i\sqrt{3};$$

$$\beta_1 = 2(\cos\pi + i\sin\pi) = -2;$$

$$\beta_2 = 2\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right) = 1 - i\sqrt{3}.$$

Racines de l'unité. Un cas particulièrement important est celui de l'extraction de la racine $n^{\text{ème}}$ de l'unité que l'on écrit sous la forme $1 = \cos 0 + i \sin 0$. Cette racine a n valeurs distinctes qui, en vertu de (4), sont toutes données par la formule

$$\sqrt[n]{1} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\,;\quad k = 0,\ 1,\ \ldots,\ n-1. \tag{6}$$

Les valeurs réelles de la racine $n^{\text{ème}}$ de l'unité correspondent à $k = 0$ et à $k = \frac{n}{2}$ si n est pair; si n est impair, il n'y a qu'une racine réelle ($k = 0$). Les nombres complexes (6) sont situés sur la circonférence de rayon 1 avec l'origine pour centre et forment un polygone régulier dont un des sommets est le nombre 1. Il en résulte que les racines $n^{\text{èmes}}$ de l'unité non réelles sont symétriques par rapport à l'axe réel, c'est-à-dire conjuguées deux à deux.

La racine carrée de l'unité a deux valeurs distinctes: 1 et -1, la racine $4^{\text{ème}}$ en a quatre: 1, -1, i et $-i$. Il est utile de retenir les trois *racines cubiques de l'unité*. D'après la formule (6), ce sont les nombres $\cos\frac{2\pi k}{3} + i\sin\frac{2\pi k}{3}$, $k = 0, 1, 2$, c'est-à-dire le nombre 1 et les nombres complexes conjugués:

$$\left.\begin{aligned} \varepsilon_1 &= \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\,\frac{\sqrt{3}}{2}, \\ \varepsilon_2 &= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\,\frac{\sqrt{3}}{2}. \end{aligned}\right\} \tag{7}$$

Toutes les racines $n^{\text{èmes}}$ d'un nombre complexe s'obtiennent en multipliant l'une de ces racines successivement par toutes les racines $n^{\text{èmes}}$ de l'unité. En effet, soit β une des racines $n^{\text{èmes}}$ de α, de sorte que $\beta^n = \alpha$, et soit ε une racine $n^{\text{ème}}$ quelconque de l'unité: $\varepsilon^n = 1$. Alors $(\beta\varepsilon)^n = \beta^n\varepsilon^n = \alpha$, c'est-à-dire $\beta\varepsilon$ est encore une racine de $\sqrt[n]{\alpha}$. Multipliant β respectivement par chaque racine $n^{\text{ème}}$ de l'unité, on obtient n racines distinctes de $\sqrt[n]{\alpha}$, c'est-à-dire toutes les racines $n^{\text{èmes}}$ de α.

Exemples. 1) L'une des racines cubiques de -8 est -2. Les deux autres sont, en vertu de (7), les nombres: $-2\varepsilon_1 = 1 - i\sqrt{3}$ et $-2\varepsilon_2 = 1 + i\sqrt{3}$ (voir l'exemple 3 ci-dessus).

2) $\sqrt[4]{81}$ a quatre valeurs: 3, -3, $3i$, $-3i$.

Si ε et η sont deux racines $n^{\text{èmes}}$ de l'unité, $\varepsilon\eta$ est encore une racine $n^{\text{ème}}$ de l'unité. En effet, $\varepsilon^n = 1$, $\eta^n = 1$, de sorte que $(\varepsilon\eta)^n = \varepsilon^n\eta^n = 1$. Ensuite, *si ε est une des racines $n^{\text{èmes}}$ de l'unité, ε^{-1} en est une aussi.* En effet, $\varepsilon^n = 1$ et $\varepsilon \cdot \varepsilon^{-1} = 1$, de sorte que $\varepsilon^n \times (\varepsilon^{-1})^n = 1$, ou encore $(\varepsilon^{-1})^n = 1$. Plus généralement, *toute puissance d'une racine $n^{\text{ème}}$ de l'unité est encore une racine $n^{\text{ème}}$ de l'unité.*

Soient l et k deux entiers quelconques. Si $\frac{k}{l}$ est entier, alors toute racine $k^{\text{ème}}$ de l'unité est aussi une des racines $l^{\text{èmes}}$ de l'unité. Il en découle que l'ensemble de toutes les racines $n^{\text{èmes}}$ de l'unité contient certaines racines $n'^{\text{èmes}}$ de l'unité, où n' est un des diviseurs de n. Néanmoins, pour tout n il existe au moins une racine $n^{\text{ème}}$, soit ε_0, telle que $\varepsilon_0^{n'} \neq 1$ quel que soit l'entier n' compris entre 0 et n: $0 < n' < n$. Une telle racine $n^{\text{ème}}$ de l'unité est dite *racine primitive*. Son existence découle de la formule (6) ; en effet, désignant par $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}$ toutes les racines $n^{\text{èmes}}$ de l'unité ($\varepsilon_0 = 1$), il vient, compte tenu de la formule de Moivre (1),

$$\varepsilon_1^k = \varepsilon_k.$$

Ainsi, $\varepsilon_1^k \neq 1$, si k est compris entre 0 et n: $0 < k < n$, de sorte que $\varepsilon_1 = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$ est effectivement une racine primitive.

Une racine $n^{\text{ème}}$ de l'unité ε est primitive si et seulement si toutes les puissances ε^k, $k = 0, 1, \ldots, n-1$, sont des nombres complexes distincts ou encore si l'ensemble $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^n$ coïncide avec l'ensemble de toutes les racines $n^{\text{èmes}}$ de l'unité.

En effet, si toutes les racines $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ sont distinctes, alors ε est évidemment une racine primitive $n^{\text{ème}}$ de l'unité. Réciproquement, si $\varepsilon^k = \varepsilon^l$ avec $0 \leqslant k < l \leqslant n-1$, alors $\varepsilon^{l-k} = 1$ avec $1 \leqslant l-k \leqslant n-1$, de sorte que ε n'est pas une racine primitive.

Le nombre ε_1 trouvé ci-dessus n'est pas la seule racine primitive. Le théorème suivant permet de trouver toutes les racines primitives $n^{\text{èmes}}$ de l'unité.

Soit ε une des racines primitives $n^{\text{èmes}}$ de l'unité. Pour que ε^k soit également une racine primitive, il faut et il suffit que k et n soient premiers entre eux.

En effet, soit d le plus grand commun diviseur des entiers k et n. Si $d > 1$ et $k = dk'$, $n = dn'$, alors

$$(\varepsilon^k)^{n'} = \varepsilon^{kn'} = \varepsilon^{k'n} = (\varepsilon^n)^{k'} = 1,$$

de sorte que ε^k n'est pas une racine primitive.

Soit, d'autre part, $d = 1$, et supposons que ε^k soit l'une des racines $m^{\text{èmes}}$ de l'unité avec $1 \leqslant m < n$. Alors

$$(\varepsilon^k)^m = \varepsilon^{km} = 1.$$

Le nombre ε étant une racine *primitive* $n^{\text{ème}}$ de l'unité, l'entier km doit être divisible par n. Etant donné que $1 \leqslant m < n$, il en résulte que k et n ont des diviseurs communs supérieurs à un, contrairement à notre hypothèse.

Ainsi, le nombre des racines primitives $n^{\text{èmes}}$ de l'unité est égal au nombre des entiers positifs k inférieurs à n et tels que k et n

soient premiers entre eux. On a l'habitude de noter ce nombre par $\varphi(n)$; l'expression de $\varphi(n)$ se trouve dans les cours de théorie des nombres.

Si p est un nombre premier, alors toutes les racines $p^{\text{èmes}}$ de l'unité, excepté le nombre 1, sont primitives. D'autre part, parmi les racines 4èmes, par exemple, les racines primitives sont i et $-i$ et non pas 1 et -1.

Chapitre V

POLYNÔMES ET LEURS ZÉROS

§ 20. Opérations sur les polynômes

Le contenu des deux premiers chapitres de ce livre, c'est-à-dire la théorie des déterminants et des systèmes d'équations linéaires, est le développement immédiat de la branche d'algèbre élémentaire qui, partant d'une équation du premier degré à une inconnue, conduit à l'étude des systèmes de deux et trois équations du premier degré, respectivement à deux et à trois inconnues. En algèbre élémentaire on attribue encore plus d'importance à une autre direction, qui consiste à passer d'une équation du premier degré à une équation du second degré et, ensuite, à certains types d'équations du troisième et du quatrième degré à une inconnue. Cette direction prend les proportions d'une branche importante, très riche en résultats, d'algèbre supérieure, qui est consacrée à l'étude des équations de degré n à une inconnue ou indéterminée. Cette branche précède du point de vue historique les autres théories algébriques; elle fait l'objet du chapitre présent et de plusieurs chapitres à venir.

La forme générale d'une équation de degré n (n étant un entier positif) est

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0. \tag{1}$$

Les coefficients a_0, a_1, . . ., a_n de cette équation sont des nombres complexes; en outre, le coefficient a_0 du terme principal est supposé non nul.

Pour l'équation (1) on pose le problème de trouver toutes ses racines. En d'autres termes, il s'agit de trouver les valeurs numériques de l'indéterminée x telles que l'équation (1) *soit satisfaite*, c'est-à-dire en remplaçant x successivement par chacune des valeurs en question et en effectuant les opérations indiquées dans le premier membre de (1), ce dernier doit s'annuler.

Il est préférable de poser un problème plus général, à savoir étudier le premier membre de l'équation (1)

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \tag{2}$$

dit *polynôme de degré n d'une indéterminée x*. Il faut avoir en vue qu'on appelle polynôme une somme finie de puissances d'expo-

sants entiers non négatifs de l'indéterminée x munies de certains coefficients numériques; il n'en est pas ainsi en algèbre élémentaire où toute somme finie de monômes est appelée polynôme. En particulier, nous ne considérons pas comme polynômes les expressions contenant des puissances d'exposants négatifs ou fractionnaires de l'indéterminée x; par exemple, les expressions $2x^2 - \frac{1}{x} + 3$, ou bien $ax^{-3} + bx^{-2} + cx^{-1} + d + ex + fx^2$, ou encore $x^{\frac{1}{2}} + 1$, ne sont pas des polynômes. Pour abréger l'écriture des polynômes on utilisera les notations $f(x)$, $g(x)$, $\varphi(x)$, etc.

Deux polynômes $f(x)$ et $g(x)$ *coïncident* (ou encore *coïncident identiquement*) : $f(x) = g(x)$, si et seulement si les coefficients des mêmes puissances de x dans les expressions de $f(x)$ et de $g(x)$ sont égaux. En particulier, tout polynôme dont au moins un des coefficients est non nul ne peut pas être égal au polynôme nul; par conséquent, le signe d'égalité qu'on utilise pour écrire une équation de degré n (1) n'a rien à voir avec la notion d'égalité de deux polynômes introduite ci-dessus. Le signe $=$ utilisé dans la suite pour établir la relation d'égalité entre les polynômes signifie que les polynômes correspondants coïncident identiquement.

Ainsi, un polynôme de degré n (2) doit être considéré comme une expression formelle bien définie quand on se donne la suite ordonnée de ses coefficients $a_0, a_1, \ldots, a_n$ avec $a_0 \neq 0$. Le sens exact de ces mots sera élucidé plus tard au chapitre X. Notons qu'en dehors de la forme (2) d'un polynôme (où les monômes sont ordonnés *suivant les puissances décroissantes de* x), on admet d'autres formes d'écriture pour les polynômes qui s'obtiennent de la forme (2) en déplaçant certains monômes; en particulier, on utilisera la forme où les monômes sont ordonnés *suivant les puissances croissantes de* x.

Evidemment, on pourrait considérer un polynôme (2) du point de vue de l'analyse, c'est-à-dire comme une fonction complexe d'une variable complexe x. Or, il faut prendre en considération que *deux fonctions ne sont égales que lorsque leurs valeurs coïncident pour toutes les valeurs de la variable* x. Il est clair que deux polynômes égaux au sens algébrique formel indiqué ci-dessus coïncident du point de vue de l'analyse en tant que fonctions de x. La réciproque ne sera démontrée qu'au § 24. Après cela, il deviendra évident que les deux points de vue, algébrique et analytique, de la notion de polynômes à coefficients numériques sont équivalents; mais pour le moment nous devons chaque fois préciser le sens qu'on attribue à la notion de polynôme. Dans ce paragraphe et dans les deux paragraphes suivants, nous considérons les polynômes comme des expressions algébriques formelles.

Il est clair que pour tout entier n il existe des polynômes de degré n. Outre les polynômes de degre un, deux, trois, etc., nous pouvons rencontrer des *polynômes de degré nul*, c'est-à-dire des nombres complexes *non nuls*. Le nombre zéro peut être également considéré comme un polynôme; c'est le seul polynôme dont le degré ne soit pas bien défini.

Maintenant, nous allons définir l'addition et la multiplication des polynômes à coefficients complexes. Ces opérations seront introduites par analogie avec les opérations correspondantes sur les polynômes à coefficients réels, connues du cours d'algèbre élémentaire.

Soient deux polynômes $f(x)$ et $g(x)$, ordonnés, pour plus de commodité, suivant les puissances croissantes de x:

$$f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n, \qquad a_n \neq 0,$$
$$g(x) = b_0 + b_1x + \ldots + b_{s-1}x^{s-1} + b_sx^s, \qquad b_s \neq 0,$$

soit, en outre, $n \geqslant s$; on appelle *somme* des polynômes $f(x)$ et $g(x)$ le polynôme

$$f(x) + g(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1} + c_nx^n,$$

dont les coefficients sont les sommes des coefficients des mêmes puissances de x dans les expressions de $f(x)$ et $g(x)$:

$$c_i = a_i + b_i, \quad i = 0, 1, \ldots, n; \tag{3}$$

si $n > s$, alors les coefficients $b_{s+1}, b_{s+2}, \ldots, b_n$ sont nuls. La somme est de degré n si $n > s$; si $n = s$, il peut arriver que la somme soit de degré inférieur à n, notamment, cela a lieu si $b_n = -a_n$.

On appelle *produit* des polynômes $f(x)$ et $g(x)$ le polynôme

$$f(x) \cdot g(x) = d_0 + d_1x + \ldots + d_{n+s-1}x^{n+s-1} + d_{n+s}x^{n+s},$$

dont les coefficients sont définis par les formules

$$d_i = \sum_{k+l=i} a_kb_l, \quad i = 0, 1, \ldots, n+s-1, n+s, \tag{4}$$

c'est-à-dire le coefficient d_i est la somme des produits de tous les coefficients a_k de $f(x)$ et b_l de $g(x)$ tels que la somme des indices $k + l$ soit égale à i; en particulier, $d_0 = a_0b_0$, $d_1 = a_0b_1 + a_1b_0$, ..., $d_{n+s} = a_nb_s$. La dernière relation a pour conséquence l'inégalité: $d_{n+s} \neq 0$, de sorte que le *degré du produit de deux polynômes est égal à la somme des degrés des facteurs.*

Il en résulte que le *produit de deux polynômes non nuls est un polynôme non nul.*

Quelles sont les propriétés dont jouissent les opérations sur les polynômes introduites ci-dessus? L'*addition est commutative et associative*, ce qui résulte immédiatement des propriétés analogues

de cette opération sur les nombres, car l'addition des polynômes se ramène à celle des coefficients des mêmes puissances de l'indéterminée. On peut *retrancher* un polynôme d'un autre, le nombre zéro jouant le rôle du polynôme *nul* et le polynôme opposé à $f(x)$ étant défini par la formule

$$-f(x) = -a_0 - a_1 x - \ldots - a_{n-1}x^{n-1} - a_n x^n.$$

La *commutativité de la multiplication* des polynômes découle de la même propriété des nombres et du fait que dans l'expression des coefficients du produit des polynômes $f(x)$ et $g(x)$ les coefficients des facteurs interviennent de façon symétrique. On peut démontrer l'*associativité de la multiplication* de la manière suivante: soit, outre les polynômes $f(x)$ et $g(x)$, encore un polynôme

$$h(x) = c_0 + c_1 x + \ldots + c_{t-1}x^{t-1} + c_t x^t, \qquad c_t \neq 0,$$

alors le coefficient de x^i, $i = 0, 1, \ldots, n+s+t$, dans l'expression du produit $[f(x)g(x)]h(x)$ est

$$\sum_{j+m=i} \Big(\sum_{k+l=j} a_k b_l\Big) c_m = \sum_{k+l+m=i} a_k b_l c_m,$$

et le coefficient de x^i dans l'expression de $f(x)[g(x)h(x)]$ est

$$\sum_{k+j=i} a_k \Big(\sum_{l+m=j} b_l c_m\Big) = \sum_{k+l+m=i} a_k b_l c_m.$$

Enfin, la *distributivité* découle de l'égalité

$$\sum_{k+l=i} (a_k + b_k) c_l = \sum_{k+l=i} a_k c_l + \sum_{k+l=i} b_k c_l,$$

le premier membre de la dernière égalité étant le coefficient de x^i dans l'expression de $[f(x) + g(x)]\,h(x)$ et le second le coefficient de x^i dans l'expression de $f(x)\,h(x) + g(x)\,h(x)$.

Notons que l'*unité* pour la multiplication est le nombre 1 considéré comme un polynôme de degré nul. D'autre part, un *polynôme* $f(x)$ *a pour inverse un polynôme* $f^{-1}(x)$ tel que

$$f(x)\,f^{-1}(x) = 1, \tag{5}$$

si et seulement si $f(x)$ *est de degré nul.* En effet, si $f(x) = a$, où a est un nombre non nul, alors $f^{-1}(x) = a^{-1}$. Si, par contre, $f(x)$ est de degré n, $n \geqslant 1$, et s'il existait un polynôme $f^{-1}(x)$ tel que (5) soit satisfait, alors le degré du premier membre de (5) serait supérieur ou égal à n, tandis que celui du second membre est nul.

Il en résulte que la *multiplication des polynômes n'a pas d'opération inverse*, c'est-à-dire que la division des polynômes, ayant pour résultat un autre polynôme, n'existe pas. De ce point de vue l'ensemble des polynômes à coefficients complexes rappelle celui des

nombres entiers. Cette analogie va assez loin, de sorte que pour les polynômes, tout comme pour les nombres entiers, il existe une *méthode de division avec reste*. Cette méthode, dans le cas des polynômes à coefficients réels, est connue du lecteur du cours d'algèbre élémentaire. Toutefois, étant donné que nous considérons à présent les polynômes à coefficients complexes, il faut donner de nouveau toutes les définitions et démonstrations nécessaires.

Pour tout couple de polynômes $f(x)$ et $g(x)$ on peut trouver un autre couple de polynômes $q(x)$ et $r(x)$ tels que

$$f(x) = g(x)\,q(x) + r(x); \tag{6}$$

en outre, le degré de $r(x)$ est strictement inférieur à celui de $g(x)$ ou bien $r(x) = 0$. Les polynômes $q(x)$ et $r(x)$ vérifiant ces conditions sont définis de façon unique.

Démontrons d'abord la seconde partie du théorème. Soit un autre couple de polynômes $\bar{q}(x)$ et $\bar{r}(x)$, vérifiant l'égalité

$$f(x) = g(x)\,\bar{q}(x) + \bar{r}(x), \tag{7}$$

où le degré de $\bar{r}(x)$ est strictement inférieur au degré de $g(x)$[1]. Les premiers membres des égalités (6) et (7) étant les mêmes, il vient

$$g(x)\,[q(x) - \bar{q}(x)] = \bar{r}(x) - r(x).$$

Le degré du second membre de cette égalité étant strictement inférieur au degré de $g(x)$, il en résulte que $q(x) - \bar{q}(x) = 0$, car, dans le cas contraire, le degré du premier membre serait supérieur ou égal au degré de $g(x)$. Donc, on a $q(x) = \bar{q}(x)$ et, par conséquent, $r(x) = \bar{r}(x)$, ce qu'il fallait démontrer.

Passons à la démonstration de la première partie du théorème. Soient n et s les degrés respectivement des polynômes $f(x)$ et $g(x)$. Si $n < s$, alors on peut poser $q(x) = 0$, $r(x) = f(x)$. Soit $n \geqslant s$; appliquons le procédé qu'on utilise en algèbre élémentaire pour la division des polynômes à coefficients réels ordonnés suivant les puissances décroissantes de l'indéterminée. Soient

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \qquad a_0 \neq 0,$$
$$g(x) = b_0x^s + b_1x^{s-1} + \ldots + b_{s-1}x + b_s, \qquad b_0 \neq 0.$$

Posant

$$f(x) - \frac{a_0}{b_0}x^{n-s}g(x) = f_1(x), \tag{8}$$

nous obtenons un polynôme dont le degré n_1 est inférieur à n. Notons le coefficient de x^{n_1} dans cette expression par a_{10}. Posons

[1] Il est possible que $\bar{r}(x) = 0$. Par la suite nous ne ferons plus de mention spéciale à ce sujet.

ensuite

$$f_1(x)-\frac{a_{10}}{b_0}x^{n_1-s}g(x)=f_2(x), \tag{8_1}$$

si on a encore $n_1 \geqslant s$ et notons par n_2 et a_{20} respectivement le degré de $f_2(x)$ et le coefficient de x^{n_2} dans l'expression de $f_2(x)$. Posons ensuite

$$f_2(x)-\frac{a_{20}}{b_0}x^{n_2-s}g(x)=f_3(x), \tag{8_2}$$

etc.

Les degrés des polynômes $f(x)$, $f_1(x)$, $f_2(x)$, ... décroissent: $n > n_1 > n_2 > \ldots$; donc, après avoir répété un nombre fini de fois ce procédé nous avons un polynôme $f_k(x)$,

$$f_{k-1}(x)-\frac{a_{k-1,0}}{b_0}x^{n_{k-1}-s}g(x)=f_k(x), \tag{8_{k-1}}$$

tel que son degré n_k soit strictement inférieur à s, ce qui arrête le processus de division. Additionnant les égalités (8), (8_1), ..., (8_{k-1}), il vient:

$$f(x)-\left(\frac{a_0}{b_0}x^{n-s}+\frac{a_{10}}{b_0}x^{n_1-s}+\ldots+\frac{a_{k-1,0}}{b_0}x^{n_{k-1}-s}\right)g(x)=f_k(x),$$

c'est-à-dire les polynômes

$$q(x)=\frac{a_0}{b_0}x^{n-s}+\frac{a_{10}}{b_0}x^{n_1-s}+\ldots+\frac{a_{k-1,0}}{b_0}x^{n_{k-1}-s},$$

$$r(x)=f_k(x)$$

vérifient, effectivement, l'égalité (6); en outre, le degré de $r(x)$ est strictement inférieur au degré de $g(x)$.

Notons que le polynôme $q(x)$ est appelé *quotient* de la division de $f(x)$ par $g(x)$ et $r(x)$ *reste* de la division.

Le procédé de division avec reste donné ci-dessus permet d'établir le résultat suivant: *si $f(x)$ et $g(x)$ sont des polynômes à coefficients réels, alors tous les polynômes $f_1(x)$, $f_2(x)$, ... et, par conséquent, le quotient $q(x)$ et le reste $r(x)$ sont des polynômes à coefficients réels.*

§ 21. Diviseurs. Plus grand commun diviseur

Soient deux polynômes non nuls à coefficients complexes $f(x)$ et $\varphi(x)$. Si le reste de la division de $f(x)$ par $\varphi(x)$ est nul, ou encore si $f(x)$ *est divisible* par $\varphi(x)$, alors le polynôme $\varphi(x)$ est appelé *diviseur* du polynôme $f(x)$.

Pour qu'un polynôme $\varphi(x)$ soit diviseur d'un autre polynôme $f(x)$, il faut et il suffit qu'il existe un polynôme $\psi(x)$ tel que l'égalité

$$f(x)=\varphi(x)\psi(x) \tag{1}$$

soit satisfaite.

En effet, si $\varphi(x)$ est un diviseur de $f(x)$, alors le polynôme $\psi(x)$ est le quotient de la division de $f(x)$ par $\varphi(x)$. Inversement, supposons qu'il existe un polynôme $\psi(x)$ tel que l'égalité (1) soit vérifiée. Nous avons démontré au paragraphe précédent l'unicité des polynômes $q(x)$ et $r(x)$ tels que l'égalité

$$f(x)=\varphi(x)\,q(x)+r(x)$$

soit vérifiée, ici le degré de $r(x)$ est inférieur à celui de $\varphi(x)$. Appliqué dans notre cas, ce résultat montre que le quotient de la division de $f(x)$ par $\varphi(x)$ est $\psi(x)$ et que le reste est nul.

Il est clair que si l'égalité (1) est vraie, alors $\psi(x)$ est encore un diviseur de $f(x)$. Bien entendu, le degré de $\varphi(x)$ n'est pas supérieur à celui de $f(x)$.

Notons que $\psi(x)$ est un polynôme à coefficients rationnels (respectivement réels) si $f(x)$ et $\varphi(x)$ sont des polynômes à coefficients rationnels (respectivement réels) ; en effet, cela résulte du procédé de division donné ci-dessus. Evidemment, un polynôme à coefficients rationnels (respectivement réels) peut avoir des diviseurs qui ne possèdent plus cette propriété, comme le montre l'exemple suivant :

$$x^2+1=(x-i)(x+i).$$

Notons quelques propriétés fondamentales de la division sans reste des polynômes, qui trouveront de multiples applications.

I. *Si $f(x)$ est divisible par $g(x)$ et si $g(x)$ est divisible par $h(x)$, alors $f(x)$ est divisible par $h(x)$.*

En effet, on a $f(x)=g(x)\,\varphi(x)$ et $g(x)=h(x)\,\psi(x)$; par conséquent, $f(x)=h(x)\,[\psi(x)\,\varphi(x)]$.

II. *Si $f(x)$ et $g(x)$ sont divisibles par $\varphi(x)$, alors il en est de même pour la somme $f(x)+g(x)$ et pour la différence $f(x)-g(x)$.*

En effet, les égalités $f(x)=\varphi(x)\,\psi(x)$ et $g(x)=\varphi(x)\,\chi(x)$ entraînent : $f(x)\pm g(x)=\varphi(x)\,[\psi(x)\pm\chi(x)]$.

III. *Si $f(x)$ est divisible par $\varphi(x)$, alors le produit $f(x)\,g(x)$, où $g(x)$ est un polynôme quelconque, est encore divisible par $\varphi(x)$.*

En effet, soit $f(x)=\varphi(x)\,\psi(x)$; alors $f(x)\,g(x)=$ $=\varphi(x)\,[\psi(x)\,g(x)]$. Des propositions II et III résulte la propriété suivante :

IV. *Si les polynômes $f_1(x)$, $f_2(x)$, . . ., $f_k(x)$ sont divisibles par $\varphi(x)$, alors le polynôme*

$$f_1(x)\,g_1(x)+f_2(x)\,g_2(x)+\ldots+f_k(x)\,g_k(x)$$

est également divisible par $\varphi(x)$, quels que soient les polynômes $g_1(x)$, $g_2(x)$, . . ., $g_k(x)$.

V. *Tout polynôme $f(x)$ est divisible par un polynôme de degré nul.*

En effet, soient $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ et c un nombre non nul (ou, ce qui revient au même, c'est un polynôme

de degré nul) ; alors on a

$$f(x) = c\left(\frac{a_0}{c}x^n + \frac{a_1}{c}x^{n-1} + \ldots + \frac{a_n}{c}\right).$$

VI. *Si $f(x)$ est divisible par $\varphi(x)$, alors $f(x)$ est divisible par $c\varphi(x)$, où c est un nombre non nul.*

En effet, l'égalité $f(x) = \varphi(x)\psi(x)$ entraîne la relation $f(x) = [c\varphi(x)]\cdot[c^{-1}\psi(x)]$.

VII. *Soit un polynôme $f(x)$; tout diviseur de $f(x)$ de même degré que $f(x)$ est de la forme: $cf(x)$, où c est un nombre, $c \neq 0$.*

En effet, $f(x) = c^{-1}[cf(x)]$, c'est-à-dire $f(x)$ est divisible par $cf(x)$.

D'autre part, si $f(x)$ est divisible par $\varphi(x)$ et si $\varphi(x)$ a le même degré que $f(x)$, alors le degré du quotient de la division de $f(x)$ par $\varphi(x)$ doit être nul, de sorte que $f(x) = d\varphi(x)$, où d est un nombre non nul; il en résulte que $\varphi(x) = d^{-1}f(x)$.

D'où découl ela propriété suivante:

VIII. *Pour que $f(x)$ et $g(x)$ soient simultanément divisibles l'un par l'autre, il faut et il suffit que $g(x) = cf(x)$, où* $c \neq 0$.

Enfin de VIII et I résulte la propriété suivante:

IX. *Tout diviseur de $f(x)$ est en même temps un diviseur de $cf(x)$, $c \neq 0$, et inversement.*

Plus grand commun diviseur. Soient deux polynômes $f(x)$ et $g(x)$. Un polynôme $\varphi(x)$ est dit *diviseur commun* de $f(x)$ et $g(x)$ si $f(x)$ et $g(x)$ sont divisibles par $\varphi(x)$. La propriété V (cf. ci-dessus) montre que pour un couple de polynômes $f(x)$ et $g(x)$ tout polynôme de degré nul est un diviseur commun. Si $f(x)$ et $g(x)$ n'ont d'autres diviseurs communs que les polynômes de degré nul. alors $f(x)$ et $g(x)$ sont dits *premiers entre eux.*

Dans le cas général, les polynômes $f(x)$ et $g(x)$ peuvent avoir des diviseurs communs qui dépendent de x; nous voulons définir *le plus grand* commun diviseur de ces polynômes.

Il serait incommode de définir le plus grand commun diviseur comme diviseur commun de degré le plus élevé de $f(x)$ et $g(x)$. En effet, nous ignorons pour le moment si une telle définition garantit l'unicité à un facteur numérique près du plus grand commun diviseur et exclut l'existence des plus grands communs diviseurs de degrés différents; en d'autres termes, nous ne savons pas encore si cette définition n'a pas un caractère trop indéterminé. D'autre part, en arithmétique le lecteur a déjà eu à faire avec le plus grand commun diviseur des nombres entiers et sait, par exemple, que le plus grand commun diviseur des nombres 12 et 18, qui est 6, est divisible par tout diviseur commun de ces nombres; en effet, les diviseurs communs de 12 et 18 sont les nombres entiers 1, 2, 3, —1, —2, —3, —6 qui sont en même temps diviseurs du nombre 6,

Ceci nous incite à adopter la définition suivante dans le cas des polynômes:

On appelle *plus grand commun diviseur* des polynômes non nuls $f(x)$ et $g(x)$ un polynôme $d(x)$ tel que $d(x)$ soit un diviseur commun de $f(x)$ et $g(x)$ et que $d(x)$ soit divisible par tout disiveur commun de $f(x)$ et $g(x)$. Le plus grand commun diviseur de $f(x)$ et $g(x)$ est noté $(f(x), g(x))$.

Cette définition laisse ouvert le problème d'existence du plus grand commun diviseur d'un couple de polynômes donnés $f(x)$ et $g(x)$. Nous allons résoudre ce problème dans le sens positif. En même temps, nous indiquerons un procédé pratique de calcul du plus grand commun diviseur d'un couple de polynômes donnés. Evidemment, nous ne pouvons pas étendre au cas des polynômes la méthode de calcul du plus grand commun diviseur de nombres entiers, puisque nous n'avons pas pour les polynômes une décomposition en produit analogue à celle des nombres entiers en un produit de nombres premiers. Néanmoins, il existe un autre moyen de trouver le plus grand commun diviseur de nombres entiers, dit *algorithme de la division successive* ou, encore, *algorithme d'Euclide*; ce procédé est valable dans le cas des polynômes.

L'algorithme d'Euclide pour les polynômes consiste dans ceci. Soient deux polynômes $f(x)$ et $g(x)$. On divise $f(x)$ par $g(x)$, ce qui donne $r_1(x)$ pour reste. On divise, ensuite, $g(x)$ par $r_1(x)$ avec $r_2(x)$ pour reste, puis on divise $r_1(x)$ par $r_2(x)$, etc. Les restes ayant les degrés décroissants, la suite des divisions successives doit aboutir inévitablement à une division sans reste et le processus s'arrêtera. *Le reste $r_k(x)$, qui est diviseur du reste précédent $r_{k-1}(x)$, est le plus grand commun diviseur des polynômes $f(x)$ et $g(x)$.*

Pour le démontrer, écrivons le processus indiqué ci-dessus sous la forme d'un système d'égalités:

$$\left.\begin{array}{r}
f(x) = g(x)\,q_1(x) + r_1(x), \\
g(x) = r_1(x)\,q_2(x) + r_2(x), \\
r_1(x) = r_2(x)\,q_3(x) + r_3(x), \\
\dots\dots\dots\dots\dots\dots \\
r_{k-3}(x) = r_{k-2}(x)\,q_{k-1}(x) + r_{k-1}(x), \\
r_{k-2}(x) = r_{k-1}(x)\,q_k(x) + r_k(x), \\
r_{k-1}(x) = r_k(x)\,q_{k+1}(x).
\end{array}\right\} \qquad (2)$$

La dernière égalité montre que $r_k(x)$ est un diviseur de $r_{k-1}(x)$. Il en résulte que les deux termes du second membre de l'avant-dernière égalité sont divisibles par $r_k(x)$ et, par conséquent, $r_k(x)$ est un diviseur de $r_{k-2}(x)$. Revenant en arrière de cette manière dans les égalités (2), nous arrivons à la conclusion que $r_k(x)$ est

un diviseur respectivement des polynômes $r_{k-3}(x), \ldots, r_2(x)$, $r_1(x)$. Il en résulte, compte tenu de la seconde égalité, que $r_k(x)$ est un diviseur de $g(x)$ et, en vertu de la première égalité, de $f(x)$. Ainsi, $r_k(x)$ est un diviseur commun de $f(x)$ et $g(x)$.

Soit maintenant $\varphi(x)$ un diviseur commun des polynômes $f(x)$ et $g(x)$. Le premier membre et le premier terme du second membre de la première égalité (2) étant divisibles par $\varphi(x)$, il en est de même pour $r_1(x)$. Passant à la seconde égalité, puis à la troisième, etc., nous obtenons de la même manière que $\varphi(x)$ est un diviseur des polynômes $r_2(x)$, $r_3(x)$, . . . Enfin, $r_{k-2}(x)$ et $r_{k-1}(x)$ étant divisibles par $\varphi(x)$, il s'ensuit de l'avant-dernière égalité que $r_k(x)$ est divisible par $\varphi(x)$. Ainsi, $r_k(x)$ est, effectivement, le plus grand commun diviseur de $f(x)$ et $g(x)$.

Ainsi, pour tout couple de polynômes, nous avons démontré l'existence du plus grand commun diviseur et indiqué le procédé permettant de le calculer. Ce procédé montre, en particulier, que *le plus grand commun diviseur de $f(x)$ et $g(x)$ est un polynôme à coefficients rationnels (respectivement réels), si les polynômes $f(x)$ et $g(x)$ sont à coefficients rationnels (respectivement réels)*, quoique ces polynômes puissent avoir d'autres diviseurs dont quelques coefficients ne sont pas rationnels (réels). Ainsi, les polynômes à coefficients rationnels

$$f(x) = x^3 - 3x^2 - 2x + 6, \quad g(x) = x^3 + x^2 - 2x - 2$$

ont le plus grand commun diviseur $x^2 - 2$ qui est un polynôme à coefficients rationnels, bien qu'ils aient également un autre diviseur commun $x - \sqrt{2}$ qui a un coefficient irrationnel.

Soit $d(x)$ le plus grand commun diviseur des polynômes $f(x)$ et $g(x)$. Alors, les propriétés VIII et IX (voir ci-dessus) montrent que $cd(x)$, où c est un nombre non nul, est également leur plus grand commun diviseur. Autrement dit, *le plus grand commun diviseur de deux polynômes est défini de façon unique à un facteur numérique non nul près*. On peut convenir que le *coefficient du terme principal dans l'expression du plus grand commun diviseur de deux polynômes doit être toujours l'unité*. Avec cette convention, on peut dire que *deux polynômes sont premiers entre eux si et seulement si leur plus grand commun diviseur est l'unité*. En effet, tout nombre non nul est le plus grand commun diviseur de deux polynômes premiers entre eux ; multipliant ce nombre par son inverse, on obtient le polynôme unité.

Exemple. Trouver le plus grand commun diviseur des polynômes

$$f(x) = x^4 + 3x^3 - x^2 - 4x - 3, \quad g(x) = 3x^3 + 10x^2 + 2x - 3.$$

Appliquant l'algorithme d'Euclide aux polynômes à coefficients entiers, nous pouvons, pour éviter les coefficients fractionnaires, multiplier $f(x)$ ou

bien diviser $g(x)$ par un nombre non nul, et cela non seulement au début de chaque division, mais aussi pendant la division. Bien entendu, cela modifiera les quotients, mais les restes (qui seuls nous intéressent) peuvent seulement se trouver multipliés par certains facteurs de degré nul. Or, cela est permis lorsqu'on calcule le plus grand commun diviseur.

Multiplions $f(x)$ par 3 et divisons le résultat par $g(x)$; il vient :

$$\begin{array}{r|l} 3x^4+9x^3-3x^2-12x-9 & 3x^3+10x^2+2x-3 \\ \cline{2-2} 3x^4+10x^3+2x^2-3x & x+1 \\ \cline{1-1} -x^3-5x^2-9x-9 & \end{array}$$

(multiplions par -3)

$$\begin{array}{r} 3x^3+15x^2+27x+27 \\ 3x^3+10x^2+2x-3 \\ \hline 5x^2+25x+30. \end{array}$$

Ainsi, le premier reste de la division est $r_1(x)=x^2+5x+6$ (nous avons divisé par 5). Divisons $g(x)$ par $r_1(x)$:

$$\begin{array}{r|l} 3x^3+10x^2+2x-3 & x^2+5x+6 \\ \cline{2-2} 3x^3+15x^2+18x & 3x-5 \\ \cline{1-1} -5x^2-16x-3 & \\ -5x^2-25x-30 & \\ \cline{1-1} 9x+27. & \end{array}$$

Le second reste de la division est donc $r_2(x)=x+3$ (nous avons divisé par 9). Etant donné que

$$r_1(x)=r_2(x)(x+2),$$

le polynôme $r_2(x)$ est le reste qui est diviseur du reste précédent. Ainsi, $r_2(x)$ est le plus grand commun diviseur cherché des polynômes $f(x)$ et $g(x)$:

$$(f(x),\ g(x))=x+3.$$

Utilisons l'algorithme d'Euclide pour démontrer le *théorème*: *Soit $d(x)$ le plus grand commun diviseur des polynômes $f(x)$ et $g(x)$. Alors il existe des polynômes $u(x)$ et $v(x)$ tels que l'on ait*

$$f(x)u(x)+g(x)v(x)=d(x). \tag{3}$$

En outre, si les degrés de $f(x)$ et de $g(x)$ sont positifs, on peut choisir $u(x)$ et $v(x)$ de manière que les degrés de $u(x)$ et de $v(x)$ soient inférieurs respectivement aux degrés de $g(x)$ et de $f(x)$.

La démonstration est basée sur les égalités (2). Etant donné que $r_k(x)=d(x)$, posons $u_1(x)=1$, $v_1(x)=-q_k(x)$; alors l'avant-dernière égalité (2) donne

$$d(x)=r_{k-2}(x)u_1(x)+r_{k-1}(x)v_1(x).$$

Mettant à la place de $r_{k-1}(x)$ son expression par $r_{k-2}(x)$ et $r_{k-3}(x)$ (voir l'égalité qui précède l'avant-dernière égalité (2)), il vient :

$$d(x)=r_{k-3}(x)u_2(x)+r_{k-2}(x)v_2(x),$$

avec $u_2(x) = v_1(x)$, $v_2(x) = u_1(x) - v_1(x)\, q_{k-1}(x)$. Continuant à revenir en arrière dans les égalités (2), nous sommes conduits à la relation (3).

Pour démontrer la seconde partie du théorème supposons que les polynômes $u(x)$ et $v(x)$, qui vérifient l'égalité (3), soient déjà trouvés, mais que, par exemple, le degré de $u(x)$ soit supérieur ou égal au degré de $g(x)$. Divisons $u(x)$ par $g(x)$:

$$u(x) = g(x)\, q(x) + r(x),$$

ici le degré de $r(x)$ est inférieur au degré de $g(x)$. Remplaçons $u(x)$ dans (3) par la dernière expression, il vient:

$$f(x)\, r(x) + g(x)\, [v(x) + f(x)\, q(x)] = d(x).$$

Le degré du facteur qui multiplie $f(x)$ est déjà inférieur au degré de $g(x)$. Le degré du polynôme entre les crochets est, à son tour, inférieur au degré de $f(x)$, car, dans le cas contraire, le degré du second terme dans le premier membre serait supérieur ou égal au degré du produit $f(x)\, g(x)$, et, le degré du premier terme étant strictement inférieur à celui de $f(x)\, g(x)$, le premier membre de la dernière égalité aurait un degré supérieur ou égal au degré de $f(x)\, g(x)$. Or, cela est impossible, le degré du polynôme $d(x)$ étant, sous nos hypothèses, strictement inférieur au degré de $f(x)\, g(x)$.

Le théorème est démontré. En même temps, nous avons le résultat suivant: si les coefficients des polynômes $f(x)$ et $g(x)$ sont rationnels (réels), alors les polynômes $u(x)$ et $v(x)$ vérifiant (3) peuvent être choisis de manière que leurs coefficients soient également rationnels (réels).

Exemple. Trouvons $u(x)$ et $v(x)$ vérifiant l'égalité (3) avec

$$f(x) = x^3 - x^2 + 3x - 10, \quad g(x) = x^3 + 6x^2 - 9x - 14.$$

Appliquons l'algorithme d'Euclide. A présent nous ne sommes plus en droit de modifier les quotients, car ils sont utilisés pour calculer les polynômes $u(x)$ et $v(x)$. Nous obtenons le système d'égalités:

$$f(x) = g(x) + (-7x^2 + 12x + 4);$$

$$g(x) = (-7x^2 + 12x + 4)\left(-\frac{1}{7}x - \frac{54}{49}\right) + \frac{235}{49}(x-2);$$

$$-7x^2 + 12x + 4 = (x-2)(-7x-2).$$

Il en résulte que $(f(x), g(x)) = x - 2$ et que

$$u(x) = \frac{7}{235}x + \frac{54}{235}, \quad v(x) = -\frac{7}{235}x - \frac{5}{235}.$$

Appliquant le théorème qui vient d'être démontré au cas de polynômes premiers entre eux, nous obtenons le résultat suivant.

Deux polynômes $f(x)$ et $g(x)$ sont premiers entre eux si et seulement si on peut trouver des polynômes $u(x)$ et $v(x)$ tels que l'égalité suivante

$$f(x)\,u(x) + g(x)\,v(x) = 1 \tag{4}$$

soit vérifiée.

On peut démontrer certains théorèmes, simples mais importants, concernant les *polynômes premiers entre eux* en s'appuyant sur ce résultat:

a) *Supposons que les couples de polynômes $f(x)$, $\varphi(x)$ et $f(x)$, $\psi(x)$ soient premiers entre eux. Alors, il en est de même pour le couple de polynômes $f(x)$, $\varphi(x)\,\psi(x)$.*

En effet, d'après (4), on peut trouver des polynômes $u(x)$ et $v(x)$ tels que l'on ait

$$f(x)\,u(x) + \varphi(x)\,v(x) = 1.$$

Multipliant cette égalité par $\psi(x)$, il vient:

$$f(x)\,[u(x)\,\psi(x)] + [\varphi(x)\,\psi(x)]\,v(x) = \psi(x),$$

d'où l'on a que tout diviseur commun de $f(x)$ et de $\varphi(x)\,\psi(x)$ serait, en même temps, un diviseur de $\psi(x)$; or, on a supposé dans l'énoncé du théorème que $(f(x), \psi(x)) = 1$.

b) *Soit $f(x)$ et $\varphi(x)$ premiers entre eux; soit un autre polynôme $g(x)$ tel que le produit $f(x)\,g(x)$ ait $\varphi(x)$ pour diviseur. Alors $g(x)$ est divisible par $\varphi(x)$.*

En effet, multipliant par $g(x)$ l'égalité

$$f(x)\,u(x) + \varphi(x)\,v(x) = 1$$

il vient:

$$[f(x)\,g(x)]\,u(x) + \varphi(x)\,[v(x)\,g(x)] = g(x).$$

Les deux termes du premier membre de cette égalité sont divisibles par $\varphi(x)$; donc, $\varphi(x)$ est un diviseur de $g(x)$.

c) *Soient $\varphi(x)$ et $\psi(x)$ deux diviseurs du polynôme $f(x)$ et supposons que $\varphi(x)$ et $\psi(x)$ soient premiers entre eux. Alors, $f(x)$ est divisible par le produit $\varphi(x)\,\psi(x)$.*

En effet, $f(x) = \varphi(x)\,\overline{\varphi}(x)$ de sorte que le produit $\varphi(x)\,\overline{\varphi}(x)$ est divisible par $\psi(x)$. Alors, d'après b), $\overline{\varphi}(x)$ est divisible par $\psi(x)$: $\overline{\varphi}(x) = \psi(x)\,\overline{\psi}(x)$, d'où $f(x) = [\varphi(x)\,\psi(x)]\,\overline{\psi}(x)$.

La définition du plus grand commun diviseur peut être étendue au cas d'une famille finie de polynômes; notamment, on appelle *plus grand commun diviseur* des polynômes $f_1(x), f_2(x), \ldots, f_s(x)$ un diviseur commun de ces polynômes tel qu'il soit divisible par tout autre diviseur commun de $f_1(x), f_2(x), \ldots, f_s(x)$. L'existence du plus grand commun diviseur pour toute famille finie de polynômes résulte du *théorème* suivant qui donne, en même temps, un moyen de le calculer.

Le plus grand commun diviseur des polynômes $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ *est égal au plus grand commun diviseur du polynôme* $f_s(x)$ *et du plus grand commun diviseur des polynômes* $f_1(x)$, $f_2(x)$, ..., $f_{s-1}(x)$.

En effet, pour $s = 2$ le théorème est évident. Supposons que le théorème soit vrai pour toute famille de $s - 1$ polynômes, de sorte que, en particulier, les polynômes $f_1(x), \ldots, f_{s-1}(x)$ possèdent un plus grand commun diviseur, soit $d(x)$. Soit $\bar{d}(x)$ le plus grand commun diviseur des polynômes $d(x)$ et $f_s(x)$. Bien entendu, $\bar{d}(x)$ est un diviseur commun de tous les polynômes donnés. D'autre part, tout autre diviseur commun de ces polynômes est, en même temps, un diviseur de $d(x)$ et, par conséquent, de $\bar{d}(x)$.

En particulier, les polynômes $f_1(x), f_2(x), \ldots, f_s(x)$ sont dits *réciproquement premiers* si leur plus grand commun diviseur est un polynôme de degré nul, c'est-à-dire si leur plus grand commun diviseur est égal à l'unité. Il peut arriver, pour $s > 2$, qu'une famille de s polynômes réciproquement premiers contienne des couples de polynômes qui ne sont pas premiers entre eux. Ainsi, les polynômes

$$f(x) = x^3 - 7x^2 + 7x + 15, \quad g(x) = x^2 - x - 20,$$
$$h(x) = x^3 + x^2 - 12x$$

sont réciproquement premiers, bien que l'on ait

$$(f(x), g(x)) = x - 5, \quad (f(x), h(x)) = x - 3, \quad (g(x), h(x)) = x + 4.$$

Le lecteur pourra, sans aucune peine, généraliser les théorèmes a)-c), démontrés ci-dessus, au cas d'une famille finie de polynômes réciproquement premiers.

§ 22. Zéros des polynômes

Nous avons déjà évoqué au § 20 le point de vue analytique de la notion de polynôme et, sous ce rapport, parlé de la valeur d'un polynôme pour une valeur particulière de x. Rappelons la définition.

Soient un polynôme

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \tag{1}$$

et un nombre c. Alors le nombre

$$f(c) = a_0c^n + a_1c^{n-1} + \ldots + a_n,$$

qui s'obtient en remplaçant x par c dans l'expression (1) de $f(x)$ et en effectuant toutes les opérations indiquées, est la *valeur du polynôme* $f(x)$ *pour* $x = c$. Bien entendu, si $f(x) = g(x)$ au sens algébrique de l'égalité des polynômes, définie au § 20, alors $f(c) = g(c)$ pour tout c.

Si

$$\varphi(x) = f(x) + g(x), \qquad \psi(x) = f(x)\,g(x),$$

il est alors facile de vérifier que

$$\varphi(c) = f(c) + g(c), \quad \psi(c) = f(c)\,g(c).$$

En d'autres termes, l'addition et la multiplication des polynômes, définies au § 20, sont les mêmes opérations sur les polynômes considérées du point de vue de la théorie des fonctions, c'est-à-dire ce sont respectivement l'addition et la multiplication des valeurs correspondantes des polynômes en tant que fonctions d'une variable.

Si $f(c) = 0$, c'est-à-dire si le polynôme $f(x)$ s'annule lorsqu'on remplace x par c, alors le nombre c est un *zéro* du polynôme $f(x)$ (ou une racine de l'équation $f(x) = 0$). Par abus de langage on dira encore que c est une racine du polynôme $f(x)$. Nous allons montrer que cette notion est en rapport direct avec la théorie de la division des polynômes développée au paragraphe précédent.

En divisant un polynôme $f(x)$ par un polynôme de degré un, on obtient le reste qui est soit un polynôme de degré nul, soit le polynôme nul. De toute façon, le reste est un nombre que nous noterons r. Divisant un polynôme $f(x)$ par le polynôme $x - c$, le théorème suivant permet de calculer le reste de la division sans être obligé d'effectuer la division.

Le reste de la division d'un polynôme $f(x)$ par $x - c$ est égal à la valeur $f(c)$ du polynôme $f(x)$ pour $x = c$.

En effet, soit

$$f(x) = (x - c)\,q(x) + r.$$

Faisant $x = c$ dans cette égalité, il vient:

$$f(c) = (c - c)\,q(c) + r = r,$$

ce qui démontre le théorème [1].

Il en découle un corollaire très important:

Pour qu'un nombre c soit zéro d'un polynôme $f(x)$, il faut et il suffit que $f(x)$ soit divisible par $x - c$.

D'autre part, si $f(x)$ est divisible par un polynôme de degré un, soit $ax + b$, alors $f(x)$ est encore divisible par $x - \left(-\frac{b}{a}\right)$, c'est-à-dire par un polynôme de la forme $x - c$. Ainsi, *le calcul des zéros d'un polynôme est équivalent au calcul de ses diviseurs de degré un.*

Pour cette raison, la méthode suivante de division d'un polynôme par $x - c$ comporte un grand intérêt, étant donné qu'elle est plus simple que le procédé général de division des polynômes. Cette

[1] Ce théorème porte le nom du mathématicien français Bezout qui était le premier à l'énoncer et à le démontrer. (*N.d.T.*)

méthode est appelée *procédé de Hörner*. Soient

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n \qquad (2)$$

et

$$f(x) = (x-c)\,q(x) + r, \qquad (3)$$

avec

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \ldots + b_{n-1}.$$

Identifiant les coefficients des mêmes puissances de x dans les deux membres de (3), il vient :

$$\begin{aligned} a_0 &= b_0, \\ a_1 &= b_1 - cb_0, \\ a_2 &= b_2 - cb_1, \\ &\ldots\ldots\ldots \\ a_{n-1} &= b_{n-1} - cb_{n-2}, \\ a_n &= r - cb_{n-1}. \end{aligned}$$

Il en résulte que $b_0 = a_0$, $b_k = cb_{k-1} + a_k$, $k = 1, 2, \ldots, n-1$; en d'autres termes, le *coefficient b_k s'obtient en multipliant par c le coefficient précédent b_{k-1} et en ajoutant ce produit au coefficient a_k*; enfin, $r = cb_{n-1} + a_n$, c'est-à-dire le reste de la division r (qui est égal en même temps à $f(c)$) s'obtient de la même façon. Ainsi, les coefficients du quotient et le reste peuvent être trouvés au moyen de calculs standard qui peuvent être ordonnés en un schéma, comme le montrent les exemples suivants :

1. Diviser $f(x) = 2x^5 - x^4 - 3x^3 + x - 3$ par $x - 3$.

Formons le tableau

$$\begin{array}{r|llllll} & 2 & -1 & -3 & 0 & 1 & -3 \\ \hline 3 & 2, & 3\cdot2-1=5, & 3\cdot5-3=12, & 3\cdot12+0=36, & 3\cdot36+1=109, & 3\cdot109-3=324 \end{array}$$

La première ligne au-dessus du trait horizontal est composée de coefficients de $f(x)$, la seconde ligne en dessous de ce trait est formée par les coefficients du quotient et par le reste, le nombre c (ici $c = 3$) se trouvant à gauche au niveau de la seconde ligne.

Ainsi, le quotient cherché est le polynôme

$$q(x) = 2x^4 + 5x^3 + 12x^2 + 36x + 109,$$

tandis que le reste $r = f(3) = 324$.

2. Diviser $f(x) = x^4 - 8x^3 + x^2 + 4x - 9$ par $x + 1$.

On a

$$\begin{array}{r|rrrrr} & 1 & -8 & 1 & 4 & -9 \\ \hline -1 & 1 & -9 & 10 & -6 & -3 \end{array}.$$

Ainsi, le quotient est

$$q(x) = x^3 - 9x^2 + 10x - 6,$$

et le reste $r = f(-1) = -3$.

Ces exemples montrent que *le procédé de Hörner peut être utilisé pour calculer la valeur d'un polynôme pour une valeur donnée de l'indéterminée x.*

Zéros multiples. On sait que si c est un zéro du polynôme $f(x)$, c'est-à-dire si $f(c) = 0$, alors $f(x)$ est divisible par $x - c$. Il peut arriver que $f(x)$ soit divisible non seulement par $x - c$, mais encore par $(x - c)$ élevé à une puissance plus grande. En tout cas, on peut trouver un entier positif k tel que $f(x)$ soit divisible par $(x - c)^k$, mais $(x - c)^{k+1}$ ne soit plus un diviseur de $f(x)$. Ainsi, on a

$$f(x) = (x - c)^k \varphi(x),$$

où $\varphi(x)$ n'est plus divisible par $x - c$, c'est-à-dire le nombre c n'est pas un zéro de $\varphi(x)$. L'entier k est dit *ordre de multiplicité* du zéro c tandis que c est dit *zéro multiple d'ordre k* du polynôme $f(x)$. Si $k = 1$, le zéro c est dit *simple*.

La notion de zéro multiple est étroitement liée à la notion de dérivée d'un polynôme. Mais nous étudions les polynômes à coefficients complexes, et nous ne pouvons donc pas utiliser la notion de dérivée introduite en analyse. La *définition* de la dérivée d'un polynôme qui suit doit être considérée comme indépendante de la définition donnée en analyse.

Soit un polynôme de degré n à coefficients complexes

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Sa *dérivée* (ou encore sa *dérivée première*) est le polynôme de degré $n - 1$:

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \ldots + 2a_{n-2}x + a_{n-1}.$$

La dérivée d'un polynôme de degré nul ou du polynôme nul est, par définition, le polynôme nul. La dérivée de la dérivée première d'un polynôme $f(x)$, notée $f''(x)$, est la *dérivée seconde* de $f(x)$, etc. Il est clair que

$$f^{(n)}(x) = n!a_0,$$

de sorte que $f^{(n+1)}(x) = 0$, c'est-à-dire *la dérivée $(n+1)^{\text{ème}}$ d'un polynôme de degré n est le polynôme nul.*

Nous ne pouvons pas utiliser dans notre cas les propriétés des dérivées qui ont été établies en analyse pour les polynômes à coefficients réels; nous devons les démontrer de nouveau pour les polynômes à coefficients complexes en partant de la définition donnée ci-dessus. Les formules de dérivation de la somme et du produit

de deux polynômes:

$$(f(x)+g(x))' = f'(x)+g'(x), \tag{4}$$

$$(f(x)\cdot g(x))' = f(x)g'(x)+f'(x)g(x), \tag{5}$$

sont ce qui nous intéresse à présent.

On établit ces formules pour $f(x)$ et $g(x)$ quelconques au moyen d'un calcul direct en partant de la définition de la dérivée ci-dessus; nous laissons au lecteur le soin de les vérifier.

La formule (5) s'étend, sans aucune peine, au cas d'un produit fini de facteurs, de sorte que l'on peut établir de cette manière la formule de dérivation de la puissance d'un polynôme

$$(f^k(x))' = kf^{k-1}(x)f'(x). \tag{6}$$

Nous nous proposons de démontrer le théorème:

Soit c un zéro multiple d'ordre k d'un polynôme $f(x)$, $k > 1$. *Alors c est un zéro multiple d'ordre* $(k-1)$ *de la dérivée première de* $f(x)$; *si* $k = 1$, *alors c n'est pas un zéro de* $f'(x)$.

En effet, soit

$$f(x) = (x-c)^k\varphi(x), \qquad k \geqslant 1, \tag{7}$$

où $\varphi(x)$ n'est plus divisible par $x-c$. Dérivant l'égalité (7), il vient:

$$f'(x) = (x-c)^k\varphi'(x) + k(x-c)^{k-1}\varphi(x) =$$
$$= (x-c)^{k-1}[(x-c)\varphi'(x) + k\varphi(x)].$$

Le premier terme de la somme entre les crochets dans le second membre est divisible par $x-c$, tandis que le second ne l'est pas; par conséquent, la somme entre les crochets n'est pas divisible par $x-c$. Etant donné que le quotient de la division de $f(x)$ par $(x-c)^{k-1}$ est bien défini, il en résulte que $(x-c)^{k-1}$ est le binôme linéaire d'exposant le plus élevé qui soit diviseur du polynôme $f'(x)$, ce qu'il fallait démontrer.

Itérant le théorème démontré ci-dessus, nous obtenons le résultat suivant: *un zéro multiple d'ordre k d'un polynôme* $f(x)$ *est un zéro multiple d'ordre* $(k-s)$ *de la dérivée* $s^{\text{ème}}$ *de* $f(x)$, *pour* $k \geqslant s$, *et n'est pas zéro de la dérivée* $k^{\text{ème}}$ *de* $f(x)$.

§ 23. Théorème fondamental

Dans le paragraphe précédent, lorsque nous avons donné la définition du zéro d'un polynôme, nous n'avons pas posé le problème d'existence d'un zéro pour un polynôme quelconque. On sait qu'il y a des polynômes à coefficients réels qui n'ont pas de zéros réels; le polynôme x^2+1 en est un exemple. On pourrait s'attendre à ce

qu'il existe des polynômes qui n'ont pas de zéros même dans l'ensemble des nombres complexes; cette éventualité paraît surtout probable si nous considérons des polynômes à coefficients complexes. S'il en était ainsi, il faudrait encore compléter l'ensemble des nombres complexes. Or, en réalité, le théorème suivant, dit *théorème fondamental de l'algèbre*, est vrai :

Tout polynôme à coefficients complexes dont le degré est supérieur ou égal à un possède au moins un zéro qui, dans le cas général, est un nombre complexe.

Ce théorème est une des plus grandes réalisations des mathématiques et trouve de multiples applications dans différents domaines de la science. En particulier, il se trouve à la base de tout le développement ultérieur de la théorie des polynômes à coefficients numériques. C'est pourquoi ce théorème est appelé « théorème fondamental de l'algèbre supérieure ». Cependant, ce théorème n'est pas un résultat purement algébrique. Toutes les méthodes de démonstration (de nombreuses furent données après la première démonstration due à Gauss, qui date du XVIII[e] siècle) utilisent, dans une mesure plus ou moins grande, les propriétés, dites topologiques, des nombres réels et complexes, qui sont étroitement liées à la notion de continuité.

Au cours de la démonstration que nous allons donner, nous considérerons le polynôme $f(x)$ à coefficients complexes comme une fonction complexe d'une variable complexe x. Ainsi, x prend les valeurs complexes, ou, encore, en tenant compte de la méthode d'introduction des nombres complexes du § 17, on peut dire que la variable x parcourt le *plan complexe*. On peut dire que les valeurs de $f(x)$ appartiennent à un autre plan complexe par analogie au cas des fonctions réelles d'une variable réelle indépendante où cette dernière parcourt l'axe des abscisses tandis que les valeurs de $f(x)$ appartiennent à un autre axe (axe des ordonnées).

La définition de la continuité d'une fonction, connue du lecteur du cours d'analyse, se généralise aux fonctions d'une variable complexe, seulement dans la définition il faut remplacer les valeurs absolues par les modules des nombres complexes.

Notamment, une fonction complexe $f(x)$ d'une variable complexe x est dite *continue en un point* x_0 si pour tout nombre réel positif ε on peut trouver un nombre réel positif δ tel que l'on ait l'inégalité

$$|f(x_0+h)-f(x_0)|<\varepsilon$$

quel que soit l'accroissement complexe h avec $|h|<\delta$. Une fonction $f(x)$ est dite *continue* si elle est continue en tout point x_0 du domaine où elle est définie; si $f(x)$ est un polynôme, ce domaine doit coïncider avec le plan complexe.

Un polynôme $f(x)$ est une fonction continue de la variable complexe x.

On peut démontrer ce théorème de la même manière qu'en analyse, notamment, en montrant que la somme et le produit de fonctions continues sont encore des fonctions continues et en remarquant que la fonction constante est continue. Nous allons donner une autre démonstration.

Démontrons d'abord le cas particulier du théorème en question, à savoir celui où le terme indépendant de x de $f(x)$ est nul. Pour cela montrons d'abord la continuité de $f(x)$ au point $x_0 = 0$. Autrement dit, démontrons le lemme (on écrit x à la place de h):

Lemme 1. *Si le terme indépendant de x d'un polynôme $f(x)$ est nul*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x,$$

c'est-à-dire si $f(0) = 0$, alors pour tout $\varepsilon > 0$ on peut choisir $\delta > 0$ tel que pour tout x avec $|x| < \delta$ on ait: $|f(x)| < \varepsilon$.

En effet, soit

$$A = \max(|a_0|, |a_1|, \ldots, |a_{n-1}|).$$

Soit ε un nombre positif donné. Montrons que si

$$\delta = \frac{\varepsilon}{A+\varepsilon}, \tag{1}$$

alors cette valeur de δ vérifie les conditions requises.

En effet,

$$|f(x)| \leqslant |a_0|\,|x|^n + |a_1|\,|x|^{n-1} + \ldots + |a_{n-1}|\,|x| \leqslant$$
$$\leqslant A(|x|^n + |x|^{n-1} + \ldots + |x|),$$

c'est-à-dire

$$|f(x)| \leqslant A\frac{|x| - |x|^{n+1}}{1-|x|}.$$

Etant donné que $|x| < \delta$ et que, d'après (1), $\delta < 1$, on a

$$\frac{|x| - |x|^{n+1}}{1-|x|} < \frac{|x|}{1-|x|},$$

de sorte que

$$|f(x)| < \frac{A|x|}{1-|x|} < \frac{A\delta}{1-\delta} = \frac{A\dfrac{\varepsilon}{A+\varepsilon}}{1-\dfrac{\varepsilon}{A+\varepsilon}} = \varepsilon,$$

ce qu'il fallait démontrer.

Etablissons maintenant la formule suivante. Soit un polynôme à coefficients complexes

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Remplaçons x par $x + h$, où h est un paramètre. Développant chaque terme $(x + h)^k$, $k \leqslant n$, du second membre, selon la formule du binôme de Newton, nous obtenons, après avoir groupé les termes des mêmes puissances de h, l'égalité suivante:

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!} f''(x) + \ldots + \frac{h^n}{n!} f^{(n)}(x),$$

dite *formule de Taylor* qui donne le développement de $f(x + h)$ suivant les puissances de l'« accroissement » h.

Maintenant la *continuité d'un polynôme $f(x)$ en un point quelconque x_0* se démontre de la manière suivante. Selon la formule de Taylor, on a

$$f(x_0 + h) - f(x_0) = c_1h + c_2h^2 + \ldots + c_nh^n = \varphi(h),$$

avec

$$c_1 = f'(x_0), \quad c_2 = \frac{1}{2!} f''(x_0), \quad \ldots, \quad c_n = \frac{1}{n!} f^{(n)}(x_0).$$

Le polynôme $\varphi(h)$ en fonction de h est un polynôme dont le terme indépendant de h est nul; il en résulte, en vertu du lemme 1, que pour tout $\varepsilon > 0$ on peut choisir $\delta > 0$ de manière que l'on ait: $|\varphi(h)| < \varepsilon$ pour $|h| < \delta$, ou encore

$$|f(x_0+h) - f(x_0)| < \varepsilon,$$

ce qu'il fallait démontrer.

L'inégalité

$$\big||f(x_0+h)| - |f(x_0)|\big| \leqslant |f(x_0+h) - f(x_0)|$$

qui découle de la formule (13) du § 18 et la continuité d'un polynôme que nous venons de démontrer prouvent que le *module* $|f(x)|$ d'un polynôme est également une *fonction continue*; le module $|f(x)|$ est manifestement une fonction, à valeurs réelles, non négatives, d'une variable complexe x.

Maintenant nous allons démontrer les lemmes qui seront ensuite utilisés pour la démonstration du théorème fondamental.

Lemme du module du terme principal d'un polynôme. *Soit un polynôme de degré n, $n \geqslant 1$, à coefficients complexes:*

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n.$$

Alors, pour tout nombre réel positif k, on a l'inégalité

$$|a_0x^n| > k\,|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n|, \tag{2}$$

pourvu que le module de l'indéterminée x soit suffisamment grand; c'est-à-dire le module du terme principal de $f(x)$ (ou le terme de plus haut degré en x) est supérieur ou égal au module de la somme des autres termes de $f(x)$ multipliée par un coefficient k arbitrairement grand et positif, à condition que le module de x soit suffisamment grand.

En effet, notons par A le plus grand des modules des nombres $a_1, a_2, \ldots, a_n$:

$$A = \max(|a_1|, |a_2|, \ldots, |a_n|).$$

Alors (cf. § 18 pour les propriétés du module de la somme et du produit de deux nombres complexes) on a

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| \leqslant |a_1| |x|^{n-1} + |a_2| |x|^{n-2} + \ldots$$
$$\ldots + |a_n| \leqslant A(|x|^{n-1} + |x|^{n-2} + \ldots + 1) = A \frac{|x|^n - 1}{|x| - 1}.$$

Si $|x| > 1$, il vient

$$\frac{|x|^n - 1}{|x| - 1} < \frac{|x|^n}{|x| - 1},$$

d'où l'on a

$$|a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| < A \frac{|x|^n}{|x| - 1}.$$

Ainsi, l'inégalité (2) est vérifiée si le module de x satisfait aux deux inégalités suivantes: $|x| > 1$ et

$$kA \frac{|x|^n}{|x| - 1} \leqslant |a_0x^n| = |a_0| |x|^n,$$

ou encore si

$$|x| \geqslant \frac{kA}{|a_0|} + 1. \tag{3}$$

Le second membre dans (3) étant plus grand que l'unité, on peut affirmer que les valeurs de x satisfaisant à (3) vérifient également l'inégalité (2), ce qui démontre le lemme.

Lemme de la croissance du module d'un polynôme. *Soit un polynôme $f(x)$ à coefficients complexes dont le degré est supérieur ou égal à l'unité. Alors pour tout nombre réel positif arbitrairement grand M on peut choisir un nombre réel positif N tel que pour $|x| > N$ on ait: $|f(x)| > M$.*

Soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n.$$

D'après la formule (11) du § 18 on a

$$|f(x)| = |a_0x^n + (a_1x^{n-1} + \ldots + a_n)| \geqslant |a_0x^n| - |a_1x^{n-1} + \ldots + a_n|. \tag{4}$$

Appliquons le lemme du module du terme principal pour $k=2$: il existe donc un nombre N_1 tel que pour $|x|>N_1$ on ait :

$$|a_0x^n|>2|a_1x^{n-1}+\ldots+a_n|.$$

Il en résulte que

$$|a_1x^{n-1}+\ldots+a_n|<\frac{1}{2}|a_0x^n|,$$

ou encore, d'après (4),

$$|f(x)|>|a_0x^n|-\frac{1}{2}|a_0x^n|=\frac{1}{2}|a_0x^n|.$$

Le second membre de la dernière inégalité est plus grand que M si

$$|x|>N_2=\sqrt[n]{\frac{2M}{|a_0|}}.$$

Ainsi, pour $|x|>N=\max(N_1, N_2)$ on a: $|f(x)|>M$.

On peut donner une interprétation géométrique de ce lemme qui sera utilisée plus d'une fois dans ce paragraphe. Supposons qu'en chaque point x_0 du plan complexe on ait construit un segment perpendiculaire au plan et de longueur, mesurée d'après une échelle donnée, égale à la valeur du module du polynôme $f(x)$ en ce point, c'est-à-dire de longueur $|f(x_0)|$. Les extrémités des perpendiculaires, en raison de la continuité du module d'un polynôme montrée ci-dessus, engendrent une surface continue située au-dessus du plan complexe. Le lemme de la croissance du module d'un polynôme montre que cette surface s'éloigne de plus en plus du plan complexe, certes d'une façon non monotone, avec la croissance de $|x_0|$. La fig. 8 représente schématiquement la courbe d'intersection de cette surface et d'un plan perpendiculaire au plan complexe et passant par un point O.

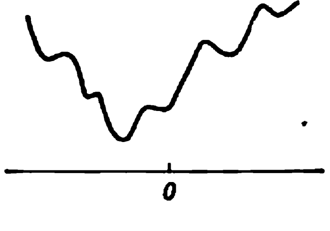


Fig. 8

Dans la démonstration du théorème fondamental le lemme suivant tient la place la plus importante :

Lemme de d'Alembert. *Soit un polynôme $f(x)$ de degré n, $n\geqslant 1$. Si pour $x=x_0$ le polynôme $f(x)$ ne s'annule pas, $f(x_0)\neq 0$ (de sorte que $|f(x_0)|>0$), alors on peut trouver un accroissement h, en général complexe, tel que l'on ait*

$$|f(x_0+h)|<|f(x_0)|.$$

On a, d'après la formule de Taylor, pour tout accroissement h:

$$f(x_0+h)=f(x_0)+hf'(x_0)+\frac{h^2}{2!}f''(x_0)+\ldots+\frac{h^n}{n!}f^{(n)}(x_0).$$

D'après notre hypothèse, le nombre x_0 n'est pas un zéro de $f(x)$. Il peut arriver éventuellement que x_0 soit un zéro de $f'(x)$ et de plusieurs autres dérivées de $f(x)$. Soit $f^{(k)}(x)$, $k \geqslant 1$, la première dérivée de $f(x)$ qui ne s'annule pas pour $x = x_0$:

$$f'(x_0)=f''(x_0)=\ldots=f^{(k-1)}(x_0)=0, \qquad f^{(k)}(x_0)\neq 0.$$

Une telle dérivée existe car

$$f^{(n)}(x_0)=n!\,a_0\neq 0,$$

où a_0 est le coefficient de x^n dans l'expression de $f(x)$. Ainsi, on a

$$f(x_0+h)=f(x_0)+\frac{h^k}{k!}f^{(k)}(x_0)+\frac{h^{k+1}}{(k+1)!}f^{(k+1)}(x_0)+\ldots+\frac{h^n}{n!}f^{(n)}(x_0).$$

Il peut arriver que certains des nombres $f^{(k+1)}(x_0), \ldots, f^{(n-1)}(x_0)$ soient également nuls, mais cela ne joue aucun rôle.

Divisant les deux membres de la dernière égalité par $f(x_0)$, $f(x_0)$ étant non nul par hypothèse, et posant

$$c_j=\frac{f^{(j)}(x_0)}{j!\,f(x_0)}, \qquad j=k, \quad k+1, \ldots, n,$$

il vient:

$$\frac{f(x_0+h)}{f(x_0)}=1+c_kh^k+c_{k+1}h^{k+1}+\ldots+c_nh^n,$$

ou encore, étant donné que $c_k\neq 0$, on a

$$\frac{f(x_0+h)}{f(x_0)}=(1+c_kh^k)+c_kh^k\left(\frac{c_{k+1}}{c_k}h+\ldots+\frac{c_n}{c_k}h^{n-k}\right).$$

Passant aux modules nous obtenons:

$$\left|\frac{f(x_0+h)}{f(x_0)}\right|\leqslant|1+c_kh^k|+|c_kh^k|\left|\frac{c_{k+1}}{c_k}h+\ldots+\frac{c_n}{c_k}h^{n-k}\right|. \tag{5}$$

Jusqu'ici nous n'avons fait aucune hypothèse sur l'accroissement h. Passons maintenant *au choix* de h; en outre le module et l'argument de h seront choisis séparément. Le module de h sera choisi de la façon suivante. L'expression

$$\frac{c_{k+1}}{c_k}h+\ldots+\frac{c_n}{c_k}h^{n-k}$$

étant un polynôme par rapport à h dont le terme indépendant de h est nul, nous pouvons, d'après le lemme 1 $\left(\text{en faisant } \varepsilon=\frac{1}{2}\right)$, trouver δ_1 tel que pour $|h|<\delta_1$ on ait

$$\left|\frac{c_{k+1}}{c_k}h+\ldots+\frac{c_n}{c_k}h^{n-k}\right|<\frac{1}{2}. \tag{6}$$

D'autre part, on a pour

$$|h| < \delta_2 = \sqrt[k]{|c_k|^{-1}}$$

l'inégalité

$$|c_k h^k| < 1. \qquad (7)$$

Supposons que le module de h vérifie l'inégalité

$$|h| < \min(\delta_1, \delta_2). \qquad (8)$$

Cela étant, l'inégalité (5) devient, en vertu de (6), une inégalite stricte:

$$\left|\frac{f(x_0+h)}{f(x_0)}\right| < |1 + c_k h^k| + \frac{1}{2}|c_k h^k|; \qquad (9)$$

la condition (7) sera utilisée plus tard.

Choisissons l'argument de h de manière que le nombre $c_k h^k$ soit réel et négatif. Autrement dit, soit

$$\arg(c_k h^k) = \arg c_k + k \arg h = \pi,$$

d'où

$$\arg h = \frac{\pi - \arg c_k}{k}. \qquad (10)$$

L'accroissement h étant choisi de cette manière, le nombre $c_k h^k$ est de signe opposé à sa valeur absolue:

$$c_k h^k = -|c_k h^k|,$$

de sorte que, utilisant l'inégalité (7), on a

$$|1 + c_k h^k| = |1 - |c_k h^k|| = 1 - |c_k h^k|.$$

Ainsi, h étant choisi d'après (8) et (10), l'inégalité (9) prend la forme

$$\left|\frac{f(x_0+h)}{f(x_0)}\right| < 1 - |c_k h^k| + \frac{1}{2}|c_k h^k| = 1 - \frac{1}{2}|c_k h^k|,$$

c'est-à-dire on a

$$\left|\frac{f(x_0+h)}{f(x_0)}\right| = \frac{|f(x_0+h)|}{|f(x_0)|} < 1,$$

d'où l'inégalité

$$|f(x_0+h)| < |f(x_0)|,$$

ce qui démontre le lemme de d'Alembert.

Utilisant l'interprétation géométrique donnée ci-dessus, on peut expliquer le lemme de d'Alembert de manière suivante. Soit $|f(x_0)| > 0$. Cela signifie que la longueur de la perpendiculaire au point x_0 du plan complexe n'est pas nulle. Alors, d'après le lemme

de d'Alembert, on peut trouver un point $x_1 = x_0 + h$ tel que $|f(x_1)| < |f(x_0)|$, c'est-à-dire un point x_1 tel que la perpendiculaire en x_1 soit plus petite que celle en x_0. Donc, la surface engendrée par les extrémités des perpendiculaires est plus proche du plan complexe au point x_1 qu'au point x_0. Il résulte de la démonstration du dernier lemme que le module de h peut être arbitrairement petit, c'est-à-dire le point x_1 peut être choisi dans un voisinage arbitrairement petit du point x_0; toutefois, cette remarque ne sera pas utilisée par la suite.

Les zéros d'un polynôme $f(x)$ sont, évidemment, des nombres complexes, ou, encore, des points du plan complexe, en lesquels la surface engendrée par les extrémités des perpendiculaires est tangente au plan complexe. On ne peut pas, en s'appuyant uniquement sur le lemme de d'Alembert, démontrer l'existence dè tels points. En effet, utilisant le lemme de d'Alembert, nous pouvons trouver une suite infinie de points $x_0, x_1, x_2, \ldots$ telle que

$$|f(x_0)| > |f(x_1)| > |f(x_2)| > \ldots \qquad (11)$$

Or, il n'en résulte pas l'existence d'un point $\bar{x}$ tel que $f(\bar{x}) = 0$; en outre, ce n'est pas toute suite décroissante de nombres réels positifs qui a pour limite le nombre zéro.

Les raisonnements qui suivent sont basés sur un théorème de la théorie des fonctions d'une variable complexe, qui généralise le théorème de Weierstrass que le lecteur connaît du cours d'analyse. Ce théorème concerne les fonctions à valeurs réelles d'une variable complexe; le module d'un polynôme en est un exemple. Pour simplifier, on parlera dans l'énoncé du théorème d'un *cercle fermé* E, en entendant par cela un cercle E du plan complexe, auquel on a ajouté la circonférence qui le délimite.

Soit une fonction à valeurs réelles $g(x)$ *d'une variable complexe* x, g *étant continue en chaque point* x *d'un cercle fermé* E *du plan complexe. Alors il existe dans* E *un point* x_0 *tel que pour tout point* x *de* E *on ait l'inégalité* $g(x) \geqslant g(x_0)$. *Donc, au point* x_0 *du cerle* E *la fonction* $g(x)$ *a un minimum.*

On peut trouver la démonstration de ce théorème dans tous les cours de théorie des fonctions d'une variable complexe, et nous ne la donnerons pas ici.

En nous bornant au cas où la fonction $g(x)$ est non négative en chaque point du cercle E (ce cas seul nous intéresse), interprétons ce théorème du point de vue géométrique déjà mentionné ci-dessus. En tout point x_0 du cercle E nous avons une perpendiculaire de longueur $g(x_0)$. Les extrémités des perpendiculaires engendrent une portion de surface continue; en outre, le cercle E étant fermé, l'existence des points qui fournissent le minimum pour cette portion de surface devient claire du point de vue géométrique. Bien entendu,

cette interprétation géométrique ne peut pas être considérée comme une démonstration rigoureuse.

Passons maintenant à la *démonstration du théorème fondamental.* Soit un polynôme $f(x)$ de degré n, $n \geqslant 1$. Notant par a_n le terme indépendant de x dans l'expression de $f(x)$, on a : $f(0) = a_n$. Appliquons au polynôme $f(x)$ le lemme de la croissance du module d'un polynôme, en posant $M = |f(0)| = |a_n|$. Donc, il existe un nombre N tel que $|f(x)| > |f(0)|$ pour $|x| > N$. Il est clair que la généralisation du théorème de Weierstrass indiquée ci-dessus est vraie pour la fonction $|f(x)|$ dans tout cercle fermé E du plan complexe. Prenons pour E le cercle fermé de rayon N et de centre au point 0. Soit x_0 un point du cercle E en lequel la fonction $|f(x)|$ a un minimum, de sorte que l'on a en particulier: $|f(x_0)| \leqslant \leqslant |f(0)|$.

Il est facile de vérifier que x_0 *est, en réalité, un point de minimum pour* $|f(x)|$ *dans tout le plan complexe.* En effet, si x' n'appartient pas à E, alors $|x'| > N$ et, par conséquent,

$$|f(x')| > |f(0)| \geqslant |f(x_0)|.$$

Enfin, il en résulte que $f(x_0) = 0$, c'est-à-dire que x_0 *est un zéro de* $f(x)$. En effet, si $f(x_0)$ n'était pas nul, alors, d'après le lemme de d'Alembert, il existerait un point x_1 tel que $|f(x_1)| < |f(x_0)|$; or, cela contredit le fait que x_0 est un point de minimum de $|f(x)|$.

Une autre démonstration du théorème fondamental de l'algèbre sera donnée au § 55.

§ 24. Conséquences du théorème fondamental

Soit un polynôme de degré n, $n \geqslant 1$, à coefficients complexes

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n. \tag{1}$$

De nouveau, nous le considérons comme une expression algébrique formelle bien définie par l'ensemble ordonné de ses coefficients. Le théorème fondamental démontré au paragraphe précédent garantit l'existence d'un zéro, réel ou complexe, soit α_1, du polynôme $f(x)$. Ainsi, le polynôme $f(x)$ peut être mis sous la forme

$$f(x) = (x - \alpha_1)\,\varphi(x).$$

Les coefficients du polynôme $\varphi(x)$ étant des nombres réels ou complexes, le même théorème permet d'affirmer l'existence d'un zéro α_2 de $\varphi(x)$, de sorte que l'on a

$$f(x) = (x - \alpha_1)(x - \alpha_2)\,\psi(x).$$

Continuant ce processus nous sommes conduits, après un nombre fini de décompositions comme ci-dessus, à la *représentation d'un polynôme* $f(x)$ *de degré* n *sous la forme d'un produit de* n *facteurs*

linéaires:

$$f(x) = a_0 (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n). \qquad (2)$$

Le produit des facteurs linéaires dans (2) est multiplié par le coefficient a_0. En effet, si ce produit était multiplié par un autre coefficient b, b étant un nombre complexe, alors développant le second membre de (2) et groupant les termes semblables, le terme principal de $f(x)$ serait bx^n et non a_0x^n, ce qui contredit l'égalité (1). Ainsi, $b = a_0$.

La représentation d'un polynôme $f(x)$ sous la forme d'un produit (2) *est définie de façon unique à l'ordre des facteurs près.*

En effet, soit encore un produit représentant $f(x)$:

$$f(x) = a_0 (x - \beta_1)(x - \beta_2) \ldots (x - \beta_n). \qquad (3)$$

(2) et (3) entraînent l'égalité

$$(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) = (x - \beta_1)(x - \beta_2) \ldots (x - \beta_n). \quad (4)$$

Si le zéro α_i était différent de tous les β_j, $j = 1, 2, \ldots, n$, alors faisant dans (4) $x = \alpha_i$ nous aurons le nombre zéro dans le premier membre et un nombre non nul dans le second.

Ainsi, *pour tout zéro α_i il y a un nombre β_j qui coïncide avec α_i et inversement.*

Il n'en résulte pas encore que les deux représentations (2) et (3) sont identiques car, parmi les zéros α_i, $i = 1, 2, \ldots, n$, il peut s'en trouver qui coïncident. Soit, par exemple, s zéros égaux à α_1 et soit, d'autre part, parmi les β_j, $j = 1, 2, \ldots, n$, t nombres β_j égaux à α_1. Il faut montrer que $s = t$.

Le degré du produit de polynômes étant égal à la somme des degrés des facteurs, le produit de deux polynômes non nuls ne peut pas être nul. Il en résulte que si deux produits de polynômes sont égaux, alors *on peut diviser les deux membres de l'égalité par le facteur commun*, c'est-à-dire si

$$f(x)\,\varphi(x) = g(x)\,\varphi(x)$$

et $\varphi(x) \neq 0$, alors l'égalité

$$[f(x) - g(x)]\,\varphi(x) = 0$$

donne

$$f(x) - g(x) = 0,$$

ou, encore,

$$f(x) = g(x).$$

Appliquons ce résultat à l'égalité (4). Soit, par exemple, $s > t$. Divisant les deux membres de (4) par le facteur commun $(x - \alpha_1)$, nous sommes amenés à l'égalité dont le premier membre contient

comme facteur une puissance non nulle de $(x - \alpha_1)$, tandis que le second membre ne possède plus de facteurs de ce type. On a déjà montré ci-dessus que cela nous conduit à une contradiction. Ainsi, l'unicité de la représentation (2) d'un polynôme $f(x)$ est démontrée.

Groupant les facteurs identiques, le produit (2) prend la forme

$$f(x) = a_0 (x-\alpha_1)^{k_1} (x-\alpha_2)^{k_2} \ldots (x-\alpha_l)^{k_l}, \tag{5}$$

où

$$k_1 + k_2 + \ldots + k_l = n.$$

A présent, on suppose que tous les zéros $\alpha_1, \alpha_2, \ldots, \alpha_l$ sont distincts.

Montrons que *le nombre entier* k_i, $i = 1, 2, \ldots, l$, *dans* (5) *est l'ordre de multiplicité du zéro* α_i *du polynôme* $f(x)$. En effet, notant par s_i l'ordre de multiplicité de α_i, on a : $s_i \geqslant k_i$. Supposons, toutefois, que $s_i > k_i$. Selon la définition de l'ordre de multiplicité d'un zéro, on a pour $f(x)$ la représentation :

$$f(x) = (x-\alpha_i)^{s_i} \varphi(x).$$

Remplaçant ici le facteur $\varphi(x)$ par sa représentation sous la forme du produit de facteurs linéaires, nous aurions pour $f(x)$ une représentation différente de (2), ce qui est en contradiction avec l'unicité de la représentation sous la forme d'un produit démontrée ci-dessus.

Ainsi, nous avons obtenu le résultat important suivant:

Tout polynôme $f(x)$ *de degré* n, $n \geqslant 1$, *à coefficients complexes, possède exactement* n *zéros, chaque zéro étant pris avec son ordre de multiplicité.*

Notons que le théorème est également vrai pour $n = 0$, car un polynôme de degré nul ne possède évidemment pas de zéros. Ce théorème n'est pas applicable *seulement* au polynôme nul qui n'a pas de degré et qui prend la valeur nulle pour toute valeur de x. Nous utiliserons cette dernière remarque dans la démonstration du *théorème*:

Soient deux polynômes $f(x)$ *et* $g(x)$ *de degré au plus* n, *qui prennent des valeurs identiques en plus de* n *points distincts. Alors* $f(x) = g(x)$.

En effet, le polynôme $f(x) - g(x)$ possède, en vertu de nos hypothèses, plus de n zéros ; son degré étant au plus n, ce polynôme est le polynôme nul: $f(x) - g(x) = 0$.

Ainsi, vu que l'ensemble des nombres distincts est infini, on peut affirmer que, *pour tout couple de polynômes distincts* $f(x)$ *et* $g(x)$, *il existe des valeurs de l'indéterminée* x, *soit* c, *telles que* $f(c) \neq g(c)$. On peut trouver ces valeurs non seulement dans l'ensemble des nombres complexes, mais aussi dans celui des nombres réels, rationnels et, même, dans celui des nombres entiers.

Ainsi, *deux polynômes à coefficients numériques, dans l'expression desquels au moins une puissance de l'indéterminée x est multipliée par des coefficients non égaux, sont des fonctions complexes différentes de la variable complexe x.* Cela démontre, finalement, *l'équivalence des deux définitions, algébrique et analytique, des polynômes à coefficients numériques données au* § 20.

Le théorème démontré ci-dessus montre qu'*un polynôme de degré au plus n est bien défini par ses valeurs en des points distincts pris arbitrairement, pourvu que le nombre de ces points soit strictement supérieur à n.* Peut-on donner arbitrairement les valeurs correspondantes d'un polynôme en ces points ? La réponse à cette question est affirmative si l'on se donne les valeurs d'un polynôme de degré n en $(n+1)$ points distincts: *il existe un polynôme de degré au plus n qui prend les valeurs données pour $n+1$ valeurs distinctes données de l'indéterminée.*

En effet, supposons que l'on veuille trouver un polynôme de degré au plus n qui prend pour $(n+1)$ valeurs distinctes de l'indéterminée x, soit $a_1, a_2, \ldots, a_{n+1}$, les valeurs $c_1, c_2, \ldots, c_{n+1}$ respectivement. Ce polynôme est donné par la formule:

$$f(x)=\sum_{i=1}^{n+1} \frac{c_i (x-a_1) \ldots (x-a_{i-1})(x-a_{i+1}) \ldots (x-a_{n+1})}{(a_i-a_1) \ldots (a_i-a_{i-1})(a_i-a_{i+1}) \ldots (a_i-a_{n+1})}. \qquad (6)$$

En effet, son degré n'est pas supérieur à n et, en outre, la valeur $f(a_i)$ est égale à c_i.

La formule (6) est dite *formule d'interpolation de Lagrange.* Le mot « interpolation » est dû à ce que, connaissant les valeurs du polynôme en $(n+1)$ points distincts, on peut calculer, d'après la formule (6), la valeur de ce polynôme en tout autre point.

Formules de Viète. Soit un polynôme de degré n dont le coefficient du terme principal est l'unité:

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n, \qquad (7)$$

et soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ ses zéros[1]. Alors $f(x)$ se met sous la forme d'un produit :

$$f(x)=(x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_n).$$

Développant le second membre et groupant les termes semblables, nous obtenons, après avoir identifié les coefficients des mêmes puissances de x dans les deux expressions de $f(x)$, les égalités, dites *formules de Viète,* qui expriment les coefficients d'un polynôme

[1] Chaque zéro est pris avec son ordre de multiplicité.

en fonction de ses zéros:

$$a_1 = -(\alpha_1 + \alpha_2 + \ldots + \alpha_n),$$
$$a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \ldots + \alpha_{n-1}\alpha_n,$$
$$a_3 = -(\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{n-1} = (-1)^{n-1}(\alpha_1\alpha_2 \ldots \alpha_{n-1} + \alpha_1\alpha_2 \ldots \alpha_{n-2}\alpha_n + \ldots + \alpha_2\alpha_3 \ldots \alpha_n),$$
$$a_n = (-1)^n \alpha_1\alpha_2 \ldots \alpha_n.$$

Ainsi, le second membre de la $k^{\text{ème}}$ égalité, $k = 1, 2, \ldots, n$, est la somme de tous les produits de k zéros, pris avec le signe $+$ ou $-$ selon que le nombre k est pair ou impair.

Lorsque $n = 2$, ces formules deviennent les relations bien connues entre les coefficients et les zéros d'un polynôme du deuxième degré. Pour $n = 3$, c'est-à-dire pour un polynôme du troisième degré, ces formules prennent la forme

$$a_1 = -(\alpha_1 + \alpha_2 + \alpha_3), \quad a_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \quad a_3 = -\alpha_1\alpha_2\alpha_3.$$

Les formules de Viète permettent de reconstituer facilement un polynôme dont on connaît les zéros. Ainsi, trouvons un polynôme $f(x)$ du quatrième degré dont deux zéros 5 et -2 sont simples et un zéro 3 d'ordre de multiplicité deux. Nous obtenons:

$$a_1 = -(5-2+3+3) = -9,$$
$$a_2 = 5\cdot(-2)+5\cdot3+5\cdot3+(-2)\cdot3+(-2)\cdot3+3\cdot3 = 17,$$
$$a_3 = -[5\cdot(-2)\cdot3+5\cdot(-2)\cdot3+5\cdot3\cdot3+(-2)\cdot3\cdot3] = 33,$$
$$a_4 = 5\cdot(-2)\cdot3\cdot3 = -90,$$

de sorte que

$$f(x) = x^4 - 9x^3 + 17x^2 + 33x - 90.$$

Si le coefficient a_0 du terme principal d'un polynôme $f(x)$ n'est pas égal à 1, alors il faut, avant d'appliquer les formules de Viète, diviser tous les coefficients du polynôme par a_0, ce qui ne modifie pas les zéros de $f(x)$. Ainsi, dans ce cas, les formules de Viète donnent les expressions des rapports des coefficients au coefficient a_0 par les zéros du polynôme.

Polynômes à coefficients réels. Maintenant, nous allons établir quelques conséquences du théorème fondamental de l'algèbre des nombres complexes, qui concernent les polynômes à coefficients réels. L'importance du théorème fondamental de l'algèbre est essentiellement due à ces conséquences.

Soit α un zéro complexe du polynôme à coefficients réels

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

c'est-à-dire on a

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0.$$

Nous savons que dans la dernière égalité on peut remplacer tous les nombres complexes par leurs conjugués. Or, les coefficients $a_0, a_1, \ldots, a_{n-1}, a_n$ de $f(x)$ et le nombre 0 du second membre étant réels, nous sommes, donc, conduits à l'égalité

$$a_0\bar{\alpha}^n + a_1\bar{\alpha}^{n-1} + \ldots + a_{n-1}\bar{\alpha} + a_n = 0$$

ou, encore,

$$f(\bar{\alpha}) = 0.$$

Ainsi, *si un nombre complexe (non réel) α est un zéro d'un polynôme $f(x)$ à coefficients réels, alors le nombre complexe conjugué $\bar{\alpha}$ l'est aussi.*

Par conséquent, le polynôme $f(x)$ est divisible par le polynôme du deuxième degré

$$\varphi(x) = (x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha}, \tag{8}$$

dont les coefficients, d'après le § 18, sont réels. Tenant compte de ceci, montrons que *les ordres de multiplicité des zéros α et $\bar{\alpha}$ du polynôme $f(x)$ sont les mêmes.*

En effet, soient k et l les ordres de multiplicité respectivement de α et de $\bar{\alpha}$ et soit, par exemple, $k > l$. Alors $f(x)$ est divisible par la puissance $l^{\text{ème}}$ du polynôme $\varphi(x)$,

$$f(x) = \varphi^l(x)\,q(x).$$

Le polynôme $q(x)$, quotient de deux polynômes à coefficients réels, est encore un polynôme à coefficients réels; or, α est un zéro d'ordre de multiplicité $(k-l)$ de $q(x)$, tandis que $\bar{\alpha}$ n'est plus un zéro de $q(x)$, ce qui est en contradiction avec le résultat démontré ci-dessus pour les polynômes à coefficients réels. Il en résulte que $k = l$.

Ainsi, nous pouvons maintenant énoncer que *les zéros complexes d'un polynôme à coefficients réels sont conjugués deux à deux.* Il s'ensuit de cette propriété et de l'unicité de la représentation (2) d'un polynôme le résultat final suivant:

Tout polynôme $f(x)$ à coefficients réels peut être représenté d'une façon unique (à l'ordre des facteurs près) sous la forme d'un produit dont les facteurs sont respectivement le coefficient a_0 du terme principal de $f(x)$, puis plusieurs polynômes à coefficients réels de degré un de la forme $x-\alpha$, correspondant aux zéros réels de $f(x)$ et, enfin, plusieurs polynômes du deuxième degré de la forme (8) *correspondant aux couples de zéros conjugués complexes.*

Pour la suite il est utile de noter que parmi les polynômes à coefficients réels avec l'unité pour coefficient du terme principal, les polynômes de degré un de la forme $x - \alpha$ et les polynômes du deuxième degré de la forme (8) sont les seuls qui ne puissent pas être mis sous la forme d'un produit de facteurs de degré plus petit; ces polynômes sont dits *irréductibles*.

§ 25*. Fractions rationnelles

Outre les polynômes, on étudie encore en analyse les fonctions dites *fractions rationnelles*; ce sont les quotients de deux polynômes $\frac{f(x)}{g(x)}$, où $g(x) \neq 0$. On effectue les opérations algébriques sur ces fonctions d'après les mêmes règles qu'en arithmétique sur les nombres rationnels, c'est-à-dire d'après les règles d'opérations sur les fractions dont les numérateurs et les dénominateurs sont entiers. L'identité de deux fonctions rationnelles, ou, encore, de deux *fractions rationnelles*, a le même sens que l'identité des fractions en arithmétique. Pour fixer les idées, nous considérons les fractions rationnelles à coefficients *réels*; le lecteur n'aura aucune peine à remarquer que tous les résultats de ce paragraphe se généralisent presque mot à mot au cas des fractions rationnelles à coefficients complexes.

Une fraction est dite *irréductible* si son numérateur et son dénominateur sont des polynômes premiers entre eux.

Toute fraction rationnelle est égale à une fraction irréductible, cette dernière étant bien définie à un facteur numérique près, ce dernier étant commun pour le dénominateur et le numérateur.

En effet, toute fraction rationnelle peut être simplifiée en divisant ses deux polynômes par leur plus grand commun diviseur, après quoi cette fraction devient irréductible. Soient deux fractions irréductibles égales $\frac{f(x)}{g(x)}$ et $\frac{\varphi(x)}{\psi(x)}$, c'est-à-dire

$$f(x)\,\psi(x) = g(x)\,\varphi(x); \tag{1}$$

alors, $f(x)$ et $g(x)$ étant premiers entre eux, il en résulte, vu la propriété b) du § 21, que $f(x)$ est un diviseur de $\varphi(x)$, tandis que, en raison de la même propriété pour $\varphi(x)$ et $\psi(x)$ (qui sont également premiers entre eux) il s'ensuit que $f(x)$ est divisible par $\varphi(x)$. Ainsi, $f(x) = c\varphi(x)$, et de (1) il résulte que $g(x) = c\psi(x)$.

Une fraction rationnelle est dite *régulière* si le degré du numérateur est inférieur à celui du dénominateur. Ajoutant à l'ensemble des fractions régulières le polynôme nul, le *théorème* suivant est vrai :

Toute fraction rationnelle peut être mise d'une façon unique sous la forme de la somme d'un polynôme et d'une fraction régulière.

En effet, soit une fraction rationnelle $\frac{f(x)}{g(x)}$ et supposons qu'en divisant $f(x)$ par $g(x)$ on obtienne l'égalité

$$f(x)=g(x)\,q(x)+r(x),$$

où le degré de $r(x)$ est inférieur à celui de $g(x)$. Alors, il est facile de vérifier que

$$\frac{f(x)}{g(x)}=q(x)+\frac{r(x)}{g(x)}.$$

Si on a également une autre égalité pour $\frac{f(x)}{g(x)}$:

$$\frac{f(x)}{g(x)}=\bar{q}(x)+\frac{\varphi(x)}{\psi(x)},$$

avec le degré de $\varphi(x)$ inférieur à celui de $\psi(x)$, alors on obtient l'égalité

$$q(x)-\bar{q}(x)=\frac{\varphi(x)}{\psi(x)}-\frac{r(x)}{g(x)}=\frac{\varphi(x)\,g(x)-\psi(x)\,r(x)}{\psi(x)\,g(x)}.$$

Le premier membre étant un polynôme et le second une fraction régulière, il en résulte que $q(x)-\bar{q}(x)=0$ et que

$$\frac{\varphi(x)}{\psi(x)}-\frac{r(x)}{g(x)}=0.$$

Les fractions rationnelles régulières peuvent être l'objet d'une étude plus détaillée. Pour cela rappelons la remarque faite à la fin du paragraphe précédent sur l'irréductibilité des polynômes de la forme $x-\alpha$ avec α réel et des polynômes de la forme $x^2 - (\beta+\bar{\beta})\,x+\beta\bar{\beta}$, où β et $\bar{\beta}$ sont deux nombres complexes conjugués. Il est facile de vérifier que dans le cas complexe les polynômes de la forme $x-\alpha$ avec α complexe jouent le même rôle.

Une fraction rationnelle régulière $\frac{f(x)}{g(x)}$ est dite *simple* si son dénominateur $g(x)$ est une puissance d'un polynôme irréductible $p(x)$,

$$g(x)=p^k(x), \qquad k\geqslant 1,$$

et le numérateur $f(x)$ de degré inférieur à celui de $p(x)$.

Le *théorème* suivant est vrai:

Toute fraction rationnelle régulière se décompose en une somme de fractions simples.

Démonstration. Soit d'abord une fraction rationnelle régulière $\frac{f(x)}{g(x)\,h(x)}$ avec les polynômes $g(x)$ et $h(x)$ premiers entre eux,

$$(g(x),\; h(x))=1.$$

Par conséquent, d'après le § 21, il existe des polynômes $\bar{u}(x)$ et $\bar{v}(x)$ tels que l'on ait

$$g(x)\bar{u}(x)+h(x)\bar{v}(x)=1.$$

Il en résulte

$$g(x)[\bar{u}(x)f(x)]+h(x)[\bar{v}(x)f(x)]=f(x). \quad (2)$$

Soit $u(x)$ le reste de la division du produit $\bar{u}(x)f(x)$ par $h(x)$, le degré de $u(x)$ étant inférieur à celui de $h(x)$. Alors l'égalité (2) peut être récrite sous la forme

$$g(x)u(x)+h(x)v(x)=f(x), \quad (3)$$

où $v(x)$ est un polynôme qui peut être facilement calculé. Les degrés du produit $g(x)u(x)$ et du polynôme $f(x)$ étant inférieurs au degré du produit $g(x)h(x)$, le degré du produit $h(x)v(x)$ est également inférieur à celui de $g(x)h(x)$, de sorte que le degré de $v(x)$ est inférieur à celui de $g(x)$. De (3) il résulte l'égalité

$$\frac{f(x)}{g(x)h(x)}=\frac{v(x)}{g(x)}+\frac{u(x)}{h(x)},$$

dont le second membre est une somme de fractions régulières.

Si au moins un des dénominateurs $g(x)$ et $h(x)$ peut être représenté sous la forme d'un produit de polynômes premiers entre eux, alors on peut réaliser encore une décomposition. Continuant ce processus nous obtiendrons *la décomposition de toute fraction régulière en une somme d'un certain nombre de fractions régulières dont chacune a pour dénominateur une puissance d'un polynôme irréductible.* Plus précisément, soit une fraction régulière $\frac{f(x)}{g(x)}$ dont le dénominateur $g(x)$ se décompose en un produit de facteurs irréductibles:

$$g(x)=p_1^{k_1}(x)p_2^{k_2}(x)\ldots p_l^{k_l}(x)$$

(on peut toujours supposer que le coefficient du terme principal du dénominateur d'une fraction rationnelle est égal à l'unité); en outre, $p_i(x)\neq p_j(x)$ pour $i\neq j$. Alors on a

$$\frac{f(x)}{g(x)}=\frac{u_1(x)}{p_1^{k_1}(x)}+\frac{u_2(x)}{p_2^{k_2}(x)}+\ldots+\frac{u_l(x)}{p_l^{k_l}(x)};$$

les termes du second membre de cette égalité sont des fractions régulières.

Il reste à considérer le cas d'une fraction régulière de la forme $\frac{u(x)}{p^k(x)}$, où $p(x)$ est irréductible. Appliquant l'algorithme de division avec reste, divisons $u(x)$ par $p^{k-1}(x)$, puis le reste de la division par $p^{k-2}(x)$, etc.

Nous sommes conduits aux égalités suivantes:

$$u(x) = p^{k-1}(x)\,s_1(x) + u_1(x),$$
$$u_1(x) = p^{k-2}(x)\,s_2(x) + u_2(x),$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$u_{k-2}(x) = p(x)\,s_{k-1}(x) + u_{k-1}(x).$$

Le degré de $u(x)$ étant, en vertu de notre hypothèse, inférieur au degré de $p^k(x)$ et les degrés des restes $u_i(x)$, $i = 1, 2, \ldots, k-1$, inférieurs aux degrés des diviseurs correspondants $p^{k-i}(x)$, les degrés de tous les quotients $s_1(x)$, $s_2(x)$, . . ., $s_{k-1}(x)$ sont strictement inférieurs au degré du polynôme $p(x)$. Le degré du dernier reste $u_{k-1}(x)$ est également inférieur à celui de $p(x)$. Il résulte des égalités obtenues que

$$u(x) = p^{k-1}(x)\,s_1(x) + p^{k-2}(x)\,s_2(x) + \ldots + p(x)\,s_{k-1}(x) + u_{k-1}(x).$$

Cela nous conduit à la représentation cherchée de la fraction rationnelle $\frac{u(x)}{p^k(x)}$ sous la forme d'une somme de fractions simples:

$$\frac{u(x)}{p^k(x)} = \frac{u_{k-1}(x)}{p^k(x)} + \frac{s_{k-1}(x)}{p^{k-1}(x)} + \ldots + \frac{s_2(x)}{p^2(x)} + \frac{s_1(x)}{p(x)}.$$

Le théorème est démontré. On peut le compléter par le *théorèm d'unicité*:

Toute fraction rationnelle régulière se décompose d'une façon unique en une somme de fractions simples.

En effet, soient deux représentations différentes d'une fraction régulière sous la forme d'une somme de fractions simples. Retranchant l'une des décompositions de l'autre et groupant les termes semblables, nous obtenons une somme de fractions simples identiquement nulle. Les dénominateurs des fractions simples formant cette somme sont certaines puissances de polynômes irréductibles distincts $p_1(x)$, $p_2(x)$, . . ., $p_s(x)$; soit $p_i^{k_i}(x)$, $i = 1, 2, \ldots, s$, la plus grande puissance du polynôme $p_i(x)$ intervenant aux dénominateurs des fractions simples. Multiplions les deux membres de l'égalité en question par le produit $p_1^{k_1-1}(x)\,p_2^{k_2}(x)\ldots p_s^{k_s}(x)$. Tous les termes de la somme, excepté un, deviennent, après cette multiplication, des polynômes. En ce qui concerne le terme $\frac{u(x)}{p_1^{k_1}(x)}$ il se transforme en une fraction dont le dénominateur est le polynôme $p_1(x)$ et le numérateur le produit $u(x)\,p_2^{k_2}(x)\ldots p_s^{k_s}(x)$. Le polynôme $p_1(x)$ étant irréductible et tout facteur du numérateur formant avec $p_1(x)$ un couple de polynômes premiers entre

eux, le numérateur n'est pas divisible par le dénominateur. Effectuant la division avec reste nous obtenons que la somme d'un polynôme et d'une fraction régulière non nulle est nulle, ce qui est impossible.

Exemple. Décomposer en une somme de fractions simples la fraction régulière réelle $\frac{f(x)}{g(x)}$ avec

$$f(x) = 2x^4 - 10x^3 + 7x^2 + 4x + 3,$$
$$g(x) = x^5 - 2x^3 + 2x^2 - 3x + 2.$$

Il est facile de vérifier que

$$g(x) = (x+2)(x-1)^2(x^2+1);$$

en outre, chacun des polynômes $x+2$, $x-1$, x^2+1 est irréductible. Il découle de la théorie exposée ci-dessus que la décomposition cherchée doit être de la forme

$$\frac{f(x)}{g(x)} = \frac{A}{x+2} + \frac{B}{(x-1)^2} + \frac{C}{x-1} + \frac{Dx+E}{x^2+1}, \tag{4}$$

où les nombres A, B, C, D et E sont à déterminer.

De (4) résulte l'égalité

$$f(x) = A(x-1)^2(x^2+1) + B(x+2)(x^2+1) + C(x+2)(x-1)(x^2+1) + Dx(x+2)(x-1)^2 + E(x+2)(x-1)^2. \tag{5}$$

Identifiant les coefficients des mêmes puissances de x dans les deux membres de l'égalité (5), nous obtenons un système de cinq équations linéaires à cinq inconnues A, B, C, D, E; en outre, il vient du théorème démontré ci-dessus que ce système possède une solution unique. Néanmoins, nous allons choisir une autre méthode.

Faisant dans (5) $x = -2$, nous avons l'égalité $45A = 135$, d'où l'on a

$$A = 3. \tag{6}$$

Faisons ensuite $x = 1$ dans (5), il vient $6B = 6$, c'est-à-dire

$$B = 1. \tag{7}$$

Maintenant, faisons dans (5) successivement $x = 0$ et $x = -1$. Utilisant (6) et (7) nous obtenons les équations

$$\left.\begin{aligned} -2C + 2E &= -2, \\ -4C - 4D + 4E &= -8. \end{aligned}\right\} \tag{8}$$

Il en résulte que

$$D = 1. \tag{9}$$

Enfin, faisons $x = 2$ dans (5). Utilisant (6), (7) et (9), nous trouvons l'équation

$$20C + 4E = -52,$$

qui, avec la première équation (8), donne

$$C = -2, \quad E = -3.$$

Ainsi,

$$\frac{f(x)}{g(x)} = \frac{3}{x+2} + \frac{1}{(x-1)^2} - \frac{2}{x-1} + \frac{x-3}{x^2+1}.$$

§ 26. Réduction d'une forme quadratique à la forme canonique

La géométrie analytique, notamment la théorie des courbes t des surfaces du second degré, se trouve à l'origine de la théorie des formes quadratiques. On sait que l'équation d'une courbe plane du deuxième degré, ayant un centre de symétrie, peut être mise, après translation de l'origine du système des coordonnées rectangulaires au centre de symétrie, sous la forme suivante:

$$Ax^2 + 2Bxy + Cy^2 = D. \qquad (1)$$

Puis, on sait qu'on peut effectuer une rotation des axes de coordonnées d'angle α, c'est-à-dire passer des coordonnées x, y aux nouvelles coordonnées x', y' :

$$\left.\begin{aligned} x &= x' \cos\alpha - y' \sin\alpha, \\ y &= x' \sin\alpha + y' \cos\alpha, \end{aligned}\right\} \qquad (2)$$

de manière que l'équation de la courbe soit réduite à la forme « canonique », le coefficient de $x'y'$ dans la forme canonique étant nul :

$$A'x'^2 + C'y'^2 = D. \qquad (3)$$

La transformation (2) peut être interprétée comme une transformation linéaire des indéterminées (cf. § 13); en outre, elle est non singulière, le déterminant de ses coefficients étant égal à l'unité. La transformation (2) étant appliquée au premier membre de l'équation (1), on peut dire que le premier membre de (1) est réduit à la forme canonique (3) par la transformation linéaire non singulière (2).

Les nombreuses applications ont nécessité le développement d'une théorie analogue dans le cas où le nombre des indéterminées est arbitraire mais fini et les coefficients sont des nombres réels ou complexes quelconques.

Généralisant l'expression qui se trouve au premier membre de l'équation (1) nous sommes amenés à introduire la notion suivante.

On appelle *forme quadratique* f de n indéterminées $x_1, x_2, \ldots, x_n$ la somme dont tout terme est le carré d'une de ces indéterminées

ou le produit de deux indéterminées distinctes. Une forme quadratique est dite *réelle* ou *complexe* selon que ses coefficients sont réels ou complexes.

Les termes semblables d'une forme quadratique étant groupés, introduisons les notations suivantes pour les coefficients de cette forme : le coefficient de x_i^2 est a_{ii} et le coefficient du produit $x_i x_j$ $2a_{ij}$, $i \neq j$ (comparer avec (1) !). Etant donné que $x_i x_j = x_j x_i$, on pourrait noter le coefficient de ce produit par $2a_{ji}$, autrement dit, les notations introduites ci-dessus sont supposées vérifier les égalités

$$a_{ji} = a_{ij}. \tag{4}$$

Cela étant, le terme $2a_{ij}x_i x_j$ peut être mis sous la forme

$$2a_{ij}x_i x_j = a_{ij}x_i x_j + a_{ji}x_j x_i,$$

et la forme quadratique f peut être représentée comme la somme de tous les termes de la forme $a_{ij}x_i x_j$, les indices i et j variant indépendamment l'un de l'autre de 1 à n :

$$f = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}x_i x_j ; \tag{5}$$

en particulier, pour $i = j$ on trouve le terme $a_{ii}x_i^2$.

Il est clair que les coefficients a_{ij} forment une matrice carrée $A = (a_{ij})$ d'ordre n ; A est appelé *matrice de la forme quadratique* f tandis que le rang r de A est dit *rang* de f. En particulier, si $r = n$, c'est-à-dire si la matrice A est non singulière, alors la forme quadratique f est dite *non singulière* (ou encore *non dégénérée*). En vertu de l'égalité (4), les éléments de la matrice A, qui sont symétriques par rapport à la diagonale principale, coïncident, de sorte que la matrice A est *symétrique*. Réciproquement, pour toute matrice symétrique A d'ordre n on peut indiquer une forme quadratique (5) de n indéterminées bien définie, ayant pour coefficients les éléments correspondants de la matrice A.

On peut récrire la forme quadratique (5), utilisant la multiplication des matrices rectangulaires, introduite au § 14. Convenons d'abord d'utiliser les notations suivantes : pour toute matrice carrée ou rectangulaire A, on désigne par A' sa matrice transposée. Si le produit des matrices A et B a un sens, alors on a :

$$(AB)' = B'A', \tag{6}$$

c'est-à-dire *la transposée du produit de deux matrices A et B est égale au produit des transposées des facteurs, l'ordre des facteurs dans ce produit étant interverti.*

En effet, supposons que le produit AB ait un sens ; alors, il est facile de vérifier que le produit $B'A'$ a également un sens, car le nombre des colonnes de la matrice B' est égal à celui des lignes de la matrice A'. L'élément de $(AB)'$, se trouvant à l'intersection

de la $i^{\text{ème}}$ ligne et de la $j^{\text{ème}}$ colonne, appartient à la $j^{\text{ème}}$ ligne et à la $i^{\text{ème}}$ colonne de la matrice AB. Il en résulte que cet élément est la somme de n produits, ayant chacun pour facteurs un élément de la $j^{\text{ème}}$ ligne de la matrice A et l'élément d'indice correspondant de la $i^{\text{ème}}$ colonne de la matrice B. Autrement dit, cet élément est égal à la somme des produits ayant pour facteurs un élément de la $j^{\text{ème}}$ colonne de la matrice A' et l'élément d'indice correspondant de la $i^{\text{ème}}$ ligne de la matrice B'. Ce qui démontre l'égalité (6).

Notons qu'*une matrice A est symétrique si et seulement si elle coïncide avec sa transposée*, c'est-à-dire si

$$A' = A.$$

Notons par X la colonne des indéterminées

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{pmatrix}$$

X est une matrice colonne à n lignes. Sa transposée est la matrice

$$X' = (x_1,\ x_2,\ \ldots,\ x_n)$$

qui est une matrice ligne à n colonnes.

A présent, la forme quadratique (5), dont la matrice des coefficients est $A = (a_{ij})$, peut être mise sous la forme d'un produit:

$$f = X'AX. \tag{7}$$

En effet, le produit AX est une matrice colonne qui est de la forme

$$AX = \begin{pmatrix} \sum\limits_{j=1}^{n} a_{1j}x_j \\ \sum\limits_{j=1}^{n} a_{2j}x_j \\ \cdot \\ \cdot \\ \cdot \\ \sum\limits_{j=1}^{n} a_{nj}x_j \end{pmatrix}.$$

Multipliant à gauche cette matrice par la matrice X' nous obtenons une « matrice » à une ligne et à une colonne, à savoir le second membre de l'égalité (5).

Effectuons une transformation linéaire des indéterminées x_1, $x_2, \ldots, x_n$, dont la matrice des coefficients est $Q = (q_{ik})$:

$$x_i = \sum_{k=1}^{n} q_{ik} y_k, \quad i = 1, 2, \ldots, n. \tag{8}$$

Que devient la forme quadratique f après cette transformation? Nous supposons les éléments de Q réels ou complexes suivant que la forme f est réelle ou complexe. Notant par Y la colonne des indéterminées $y_1, y_2, \ldots, y_n$, représentons la transformation linéaire (8) sous la forme de l'égalité matricielle:

$$X = QY. \tag{9}$$

On a, en vertu de (6),

$$X' = Y'Q'. \tag{10}$$

Substituant dans (7) à X et X' leurs expressions (9) et (10), il vient:

$$f = Y'(Q'AQ)Y,$$

ou encore

$$f = Y'BY,$$

avec

$$B = Q'AQ.$$

Tenant compte de l'égalité (6), valable pour un nombre quelconque de facteurs, et étant donné que la matrice A est symétrique (ce qui est équivalent à l'égalité $A' = A$), il vient:

$$B' = Q'A'Q = Q'AQ = B,$$

c'est-à-dire la matrice B est également symétrique. Ainsi nous avons démontré le théorème suivant:

Une forme quadratique de n indéterminées ayant pour matrice de ses coefficients une matrice A devient, après une transformation linéaire des indéterminées, de matrice Q, une forme quadratique des nouvelles indéterminées de matrice des coefficients $Q'AQ$.

Supposons à présent que la transformation linéaire soit *non singulière*, c'est-à-dire que Q et, par conséquent, Q' soient des matrices non singulières. Les résultats du § 14 montrent que le rang du produit $Q'AQ$ est égal à celui de la matrice A. Ainsi, *le rang d'une forme quadratique est conservé lorsque les indéterminées sont soumises à une transformation linéaire non dégénérée.*

Considérons à présent, par analogie au problème géométrique de réduction de l'équation d'une courbe plane du deuxième degré ayant un centre de symétrie à la forme canonique (3) indiqué au

début de ce paragraphe, le problème de réduction d'une forme quadratique quelconque au moyen d'une transformation linéaire non singulière à la somme de carrés des indéterminées, c'est-à-dire à une forme, dite *canonique*, où les coefficients des produits d'indéterminées distinctes sont nuls. Supposons d'abord qu'une forme quadratique f de n indéterminées $x_1, x_2, \ldots, x_n$ soit déjà réduite par une transformation linéaire non dégénérée à la forme canonique

$$f = b_1y_1^2 + b_2y_2^2 + \ldots + b_ny_n^2, \tag{11}$$

$y_1, y_2, \ldots, y_n$ étant les nouvelles indéterminées. Evidemment, certains des coefficients $b_1, b_2, \ldots, b_n$ peuvent être nuls. Montrons que *le nombre de coefficients non nuls dans* (11) *est égal au rang r de la forme f.*

En effet, la forme (11) ayant été obtenue à la suite d'une transformation non singulière, la forme quadratique, qui se trouve au second membre de l'égalité (11), doit être de rang r. Or, la matrice de cette forme quadratique est une matrice diagonale

$$\begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix},$$

et elle est de rang r si et seulement si sa diagonale principale contient exactement r éléments non nuls.

Passons maintenant à la démonstration du *théorème fondamental des formes quadratiques.*

Toute forme quadratique peut être réduite, au moyen d'une transformation linéaire non singulière, à la forme canonique. En outre, si la forme quadratique est réelle, alors les coefficients de la matrice de la transformation linéaire peuvent être choisis réels.

Ce théorème est évidemment valable pour les formes quadratiques d'une indéterminée, car une telle forme quadratique ne contient qu'un terme de la forme ax^2 et, par conséquent, est déjà réduite à la forme canonique. Nous pouvons donc faire la démonstration par récurrence sur le nombre des indéterminées n, c'est-à-dire démontrer le théorème pour les formes quadratiques de n indéterminées en supposant qu'il soit vrai pour les formes quadratiques dont le nombre des indéterminées est inférieur à n.

Soit une forme quadratique de n indéterminées $x_1, x_2, \ldots, x_n$

$$f = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}x_ix_j. \tag{12}$$

Essayons de trouver une transformation linéaire non dégénérée telle que l'une des nouvelles indéterminées dans l'expression de f soit séparée des autres, c'est-à-dire une transformation qui réduise f à la somme de deux termes dont l'un est le carré de l'une des indéterminées nouvelles, soit y_1^2, et l'autre est une forme quadratique des indéterminées $y_2, \ldots, y_n$. Ce but peut être aisément atteint, si les coefficients $a_{11}, a_{22}, \ldots, a_{nn}$, éléments diagonaux de la matrice de la forme f, ne sont pas tous nuls, c'est-à-dire si l'expression (12) contient au moins une indéterminée x élevée au carré avec un coefficient non nul.

Soit, par exemple, $a_{11} \neq 0$. Alors, il est facile de vérifier que la forme quadratique $a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)^2$ a exactement les mêmes termes en x_1 que la forme quadratique f, de sorte que la différence

$$f - a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)^2 = g$$

est une forme quadratique seulement des indéterminées $x_2, \ldots, x_n$. Il en résulte que

$$f = a_{11}^{-1}(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n)^2 + g.$$

Notant

$$y_1 = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \quad y_i = x_i, \text{ avec } i = 2, 3, \ldots, n, \tag{13}$$

il vient :

$$f = a_{11}^{-1}y_1^2 + g, \tag{14}$$

g étant une forme quadratique des indéterminées $y_2, y_3, \ldots, y_n$. L'expression (14) est la formule cherchée pour la forme quadratique f, car nous l'avons obtenue de l'expression (12) par une transformation linéaire non dégénérée des indéterminées $x_1, x_2, \ldots, x_n$. Notamment, cette transformation est l'inverse de la transformation linéaire (13) à déterminant $a_{11} \neq 0$, qui est donc non dégénérée.

Si, par contre, on a $a_{11} = a_{22} = \ldots = a_{nn} = 0$, alors il faut effectuer d'abord une transformation auxiliaire des indéterminées de manière qu'elle fasse apparaître le carré de l'une des indéterminées dans l'expression de f. Les coefficients a_{ij} dans l'expression (12) n'étant pas tous nuls (si $a_{ij} = 0$ pour tous les i et j, la forme $f = 0$), on peut supposer, sans restreindre la généralité, que $a_{12} \neq 0$. Cela étant, la forme f est la somme du terme $2a_{12}x_1x_2$ et d'une expression dont chaque terme contient au moins l'une des indéterminées $x_3, \ldots, x_n$.

Soumettons maintenant les indéterminées à une transformation linéaire de la forme

$$x_1 = z_1 - z_2, \quad x_2 = z_1 + z_2, \quad x_i = z_i \text{ pour } i = 3, \ldots, n. \tag{15}$$

Elle est non dégénérée, car son déterminant est

$$\begin{vmatrix} 1 & -1 & 0 & \dots & 0 \\ 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix} = 2 \neq 0.$$

Après cette transformation le terme $2a_{12}x_1x_2$ de f prend la forme

$$2a_{12}x_1x_2 = 2a_{12}(z_1 - z_2)(z_1 + z_2) = 2a_{12}z_1^2 - 2a_{12}z_2^2,$$

c'est-à-dire la forme f contiendra z_1^2 et z_2^2 avec les coefficients non nuls, car tous les autres termes contiennent chacun au moins une des indéterminées $z_3, \dots, z_n$, de sorte que z_1^2 ni z_2^2 ne peuvent pas disparaître. A présent, nous avons la même situation que dans le cas déjà considéré ci-dessus, c'est-à-dire appliquant encore une transformation linéaire non dégénérée, nous pouvons réduire f à la forme (14).

Maintenant, il suffit de noter que g est une forme quadratique contenant au plus $n - 1$ indéterminées de sorte qu'en vertu de l'hypothèse de récurrence on peut la réduire par une transformation linéaire non dégénérée des indéterminées $y_2, y_3, \dots, y_n$ à la forme canonique. Cela achève la démonstration, car cette transformation, considérée comme une transformation des indéterminées $y_1, y_2, \dots, y_n$ (qui conserve y_1) est, bien entendu, non dégénérée et réduit la forme (14) à la forme canonique. Ainsi, la forme quadratique f peut être réduite par deux, tout au plus trois transformations linéaires non dégénérées (on peut remplacer ces transformations par une seule, qui est leur produit), à la somme de carrés des indéterminées avec certains coefficients. On sait que le nombre de ces carrés est égal au rang r de la forme f. Si, en plus, la forme quadratique f est réelle, alors les coefficients de la forme canonique, ainsi que les coefficients de la transformation linéaire qui réduit f, sont également réels; en effet, les coefficients de la transformation inverse de (13), ainsi que les coefficients de la transformation (15) sont réels.

La démonstration du théorème fondamental est achevée. On peut l'utiliser dans des exemples concrets pour réduire les formes quadratiques à la forme canonique. Seulement, au lieu de la récurrence sur le nombre des indéterminées, il faut appliquer successivement le procédé ci-dessus, faisant apparaître les carrés des indéterminées.

Exemple. Réduire à la forme canonique la forme quadratique

$$f = 2x_1x_2 - 6x_2x_3 + 2x_3x_1. \tag{16}$$

La forme f ne contenant pas de carrés des indéterminées, réalisons d'abord la transformation linéaire non dégénérée

$$x_1=y_1-y_2,\quad x_2=y_1+y_2,\quad x_3=y_3$$

à matrice

$$A=\begin{pmatrix}1 & -1 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix};$$

il vient :

$$f=2y_1^2-2y_2^2-4y_1y_3-8y_2y_3.$$

Le coefficient de y_1^2 étant non nul, on peut séparer, dans l'expression de f, l'une des indéterminées. Faisant

$$z_1=2y_1-2y_3,\quad z_2=y_2,\quad z_3=y_3,$$

c'est-à-dire réalisant une transformation linéaire dont l'inverse a pour matrice la matrice

$$B=\begin{pmatrix}\frac{1}{2} & 0 & 1\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

nous réduisons f à la forme

$$f=\frac{1}{2}z_1^2-2z_2^2-2z_3^2-8z_2z_3.$$

Nous avons séparé seulement l'indéterminée z_1, car la forme contient encore le produit des deux autres indéterminées. Le coefficient de z_2^2 étant non nul, nous pouvons utiliser encore une fois la méthode ci-dessus. Effectuant la transformation linéaire

$$t_1=z_1,\quad t_2=-2z_2-4z_3,\quad t_3=z_3,$$

dont l'inverse a pour matrice

$$C=\begin{pmatrix}1 & 0 & 0\\ 0 & -\frac{1}{2} & -2\\ 0 & 0 & 1\end{pmatrix},$$

nous sommes, finalement, conduits à la forme canonique de f :

$$f=\frac{1}{2}t_1^2-\frac{1}{2}t_2^2+6t_3^2. \qquad (17)$$

La transformation linéaire, réduisant la forme (16) à la forme canonique (17), a pour matrice le produit des matrices A, B et C

$$ABC=\begin{pmatrix}\frac{1}{2} & \frac{1}{2} & 3\\ \frac{1}{2} & -\frac{1}{2} & -1\\ 0 & 0 & 1\end{pmatrix}.$$

On peut, d'ailleurs, vérifier directement que la transformation linéaire non dégénérée $\left(\text{son déterminant est } -\frac{1}{2}\right)$

$$\begin{aligned} x_1 &= \frac{1}{2} t_1 + \frac{1}{2} t_2 + 3t_3, \\ x_2 &= \frac{1}{2} t_1 - \frac{1}{2} t_2 - t_3, \\ x_3 &= \qquad\qquad\quad t_3 \end{aligned}$$

réduit la forme (16) à la forme (17).

La réduction des formes quadratiques à la forme canonique est analogue à la réduction des équations des courbes du deuxième degré à centre de symétrie en géométrie analytique; pourtant, notre théorie ne saurait être considérée comme une généralisation de la théorie géométrique. En effet, notre théorie admet toutes les transformations linéaires non dégénérées, tandis que la réduction des équations des courbes du deuxième degré à la forme canonique se fait par l'application des transformations linéaires très spéciales du type (2) qui sont des rotations du plan. Néanmoins, on peut généraliser cette théorie géométrique au cas des formes quadratiques de n indéterminées à coefficients *réels*. La théorie géométrique des formes de n indéterminées fait l'objet du chapitre VIII et nous l'appelons *réduction d'une forme quadratique à ses axes principaux*.

§ 27. Théorème d'inertie

La forme canonique n'est pas définie de façon unique: une forme quadratique peut avoir plusieurs formes canoniques différentes en fonction de la transformation linéaire qui la réduit. Ainsi, la forme quadratique $f = 2x_1x_2 - 6x_2x_3 + 2x_3x_1$, considérée au paragraphe précédent, est réductible par la transformation linéaire non dégénérée

$$\begin{aligned} x_1 &= t_1 + 3t_2 + 2t_3, \\ x_2 &= t_1 - t_2 - 2t_3, \\ x_3 &= \qquad t_2 \end{aligned}$$

à la forme canonique

$$f = 2t_1^2 + 6t_2^2 - 8t_3^2,$$

qui est différente de celle obtenue précédemment.

On peut s'interroger qu'y a-t-il de commun entre les différentes formes canoniques d'une forme quadratique donnée f. Ce problème est très étroitement lié, comme on le verra plus tard, au problème suivant: soient deux formes quadratiques; quelle est la condition

qui permet de transformer l'une en l'autre par une transformation linéaire non dégénérée des indéterminées? Selon que l'on considère les formes quadratiques réelles ou complexes, la solution de ces problèmes n'est pas la même.

Supposons d'abord que les formes quadratiques considérées soient *complexes* et que l'on admette également les transformations linéaires non dégénérées à coefficients complexes. Nous savons que toute forme quadratique f de n indéterminées, de rang r, est réductible à la forme canonique

$$f = c_1 y_1^2 + c_2 y_2^2 + \ldots + c_r y_r^2,$$

où tous les coefficients $c_1, c_2, \ldots, c_r$ sont non nuls. Etant donné qu'on peut extraire la racine carrée de tout nombre complexe, réalisons la transformation linéaire non dégénérée:

$$z_i = \sqrt{c_i}\, y_i \quad \text{pour} \quad i = 1, 2, \ldots, r; \; z_j = y_j \quad \text{pour} \quad j = r+1, \ldots, n.$$

Elle réduit f à la forme

$$f = z_1^2 + z_2^2 + \ldots + z_r^2, \tag{1}$$

dite *normale*; la forme normale d'une forme quadratique est la somme des carrés de r indéterminées avec les coefficients égaux à l'unité.

La forme normale ne dépend que du rang r de la forme f, c'est-à-dire toutes les formes quadratiques de même rang r sont réductibles à la même forme normale (1). Par conséquent, si les formes f et g sont de même rang r, alors on peut réduire f à la forme (1) et, ensuite, transformer la forme (1) en g; autrement dit, il existe une transformation linéaire non dégénérée qui transforme f en g. Comme, d'autre part, toute transformation linéaire non dégénérée conserve le rang d'une forme quadratique, nous sommes conduits au résultat suivant:

Deux formes quadratiques complexes de n indéterminées sont réductibles l'une à l'autre par une transformation linéaire non dégénérée à coefficients complexes si et seulement si ces formes sont de même rang.

Il résulte de ce théorème qu'*une forme quadratique complexe de rang r est réductible à la forme canonique comprenant les carrés de r indéterminées avec les coefficients complexes arbitraires non nuls.*

La situation est un peu plus compliquée si l'on considère les formes quadratiques *réelles* et si, en plus, l'on n'admet que les transformations linéaires à coefficients réels (c'est surtout la seconde condition qui est importante). Ce n'est pas toute forme quadratique qui est réductible, dans ce cas, à la forme (1), car, sur cette voie, nous pouvons nous heurter au problème d'extraction de la racine carrée d'un nombre négatif. Si, toutefois, nous appelons à présent *forme normale* d'une forme quadratique f la somme des carrés des

indéterminées avec les coefficients $+1$, -1 ou 0, alors nous pouvons énoncer le résultat suivant: *toute forme quadratique réelle f est réductible au moyen d'une transformation linéaire non dégénérée à coefficients réels à la forme normale.*

En effet, la forme f de rang r des indéterminées $x_1, x_2, \ldots, x_n$ est réductible à la forme canonique, c'est-à-dire les indices des indéterminées étant convenablement choisis, on peut mettre f sous la forme

$$f = c_1 y_1^2 + \ldots + c_k y_k^2 - c_{k+1} y_{k+1}^2 - \ldots - c_r y_r^2, \qquad 0 \leqslant k \leqslant r,$$

avec $c_1, c_2, \ldots, c_k$; $c_{k+1}, \ldots, c_r$ réels et positifs. Cela étant, la transformation linéaire non dégénérée à coefficients réels

$$z_i = \sqrt{c_i}\, y_i \quad \text{pour} \quad i = 1, 2, \ldots, r, \; z_j = y_j \quad \text{pour} \quad j = r+1, \ldots, n,$$

réduit f à la forme normale

$$f = z_1^2 + \ldots + z_k^2 - z_{k+1}^2 - \ldots - z_r^2.$$

Le nombre total des carrés, intervenant dans le second membre, est égal au rang de la forme quadratique.

Une forme quadratique réelle peut être réduite à la forme normale par une multitude de transformations différentes. Néanmoins, la forme normale est définie de façon unique (à l'ordre des indéterminées près). Cela résulte du théorème très important, dit *théorème d'inertie des formes quadratiques réelles*:

Le nombre de coefficients positifs, négatifs ou nuls, intervenant dans la forme normale d'une forme quadratique réelle, ne dépend pas du choix de la transformation linéaire non dégénérée à coefficients réels qui la réduit.

En effet, soient deux formes normales d'une forme quadratique réelle f de rang r des indéterminées $x_1, x_2, \ldots, x_n$:

$$\begin{aligned} f &= y_1^2 + \ldots + y_k^2 - y_{k+1}^2 - \ldots - y_r^2 = \\ &= z_1^2 + \ldots + z_l^2 - z_{l+1}^2 - \ldots - z_r^2. \end{aligned} \tag{2}$$

Le passage des indéterminées $x_1, x_2, \ldots, x_n$ aux indéterminées $y_1, y_2, \ldots, y_n$ étant une transformation linéaire non dégénérée, il en résulte que la transformation inverse (le passage des indéterminées y_i aux indéterminées x_i)

$$y_i = \sum_{s=1}^{n} a_{is} x_s, \qquad i = 1, 2, \ldots, n, \tag{3}$$

est également non dégénérée. De même,

$$z_j = \sum_{t=1}^{n} b_{jt} x_t, \qquad j = 1, 2, \ldots, n, \tag{4}$$

où le déterminant des coefficients b_{jt} est non nul. En outre, les coefficients des transformations (3) et (4) sont réels.

Supposons maintenant que $k < l$; écrivons les égalités

$$y_1 = 0, \ldots, y_k = 0, \ z_{l+1} = 0, \ldots, z_r = 0, \ldots, z_n = 0. \qquad (5)$$

Remplaçant les premiers membres de ces égalités par leurs expressions (3) et (4), nous obtenons un système de $n - l + k$ équations linéaires homogènes par rapport aux inconnues $x_1, x_2, \ldots, x_n$. Le nombre d'équations étant strictement inférieur au nombre d'inconnues, le système (5), en vertu du § 1, possède une solution réelle *non nulle*, soit $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Remplaçons, maintenant, dans (2) tous les y_i et z_j par leurs expressions (3) et (4) et substituons, ensuite, à la place des inconnues $x_1, x_2, \ldots, x_n$ les nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$. Soient $y_i(\alpha)$ et $z_j(\alpha)$ les valeurs correspondantes de y_i et z_j; en vertu de (5), l'identité (2) prend la forme

$$-y_{k+1}^2(\alpha) - \ldots - y_r^2(\alpha) = z_1^2(\alpha) + \ldots + z_l^2(\alpha). \qquad (6)$$

Les coefficients des égalités (3) et (4) étant réels, tous les carrés dans (6) sont positifs, de sorte que tous ces carrés sont nuls; on en déduit les égalités

$$z_1(\alpha) = 0, \ \ldots, \ z_l(\alpha) = 0. \qquad (7)$$

D'autre part, en vertu du choix des nombres $\alpha_1, \alpha_2, \ldots, \alpha_n$, on a

$$z_{l+1}(\alpha) = 0, \ \ldots, \ z_r(\alpha) = 0, \ \ldots, \ z_n(\alpha) = 0. \qquad (8)$$

Ainsi, le système de n équations linéaires homogènes à n inconnues

$$z_i = 0, \quad i = 1, 2, \ldots, n,$$

possède, selon (7) et (8), une solution non triviale $\alpha_1, \alpha_2, \ldots, \alpha_n$; par conséquent, le déterminant de ce système est nul. Or, cela est contraire à l'hypothèse que la transformation (4) est non dégénérée. Nous nous heurtons à la même contradiction si nous supposons que $l < k$, d'où l'égalité $k = l$, qui démontre le théorème.

Le nombre de coefficients positifs et négatifs de la forme normale d'une forme quadratique réelle f est dit respectivement *indice d'inertie positif* et *négatif* de la forme f, tandis que la différence de ces indices est appelée *signature* de la forme f. Bien entendu, si le rang d'une forme est donné et si l'on connaît, en plus, l'un des trois nombres définis ci-dessus, alors on peut trouver les deux autres, de sorte que nous ne parlerons dans l'énoncé des théorèmes que de l'un de ces nombres.

Démontrons maintenant le théorème:

Soient deux formes quadratiques de n indéterminées à coefficients réels; on peut les réduire l'une à l'autre par une transformation linéaire

réelle non dégénérée si et seulement si ces deux formes sont de même rang et de même signature.

En effet, supposons qu'une forme f est réductible à la forme g par une transformation réelle non dégénérée. On sait que cette transformation conserve le rang de la forme. Elle conserve aussi la signature, car, dans le cas contraire, les formes f et g auraient des formes normales différentes, de sorte que la forme f serait réductible à ces deux formes normales. Or, cela contredit le théorème d'inertie. Inversement, si les formes f et g sont de même rang et de même signature, alors elles sont réductibles toutes deux à une même forme normale et, par conséquent, peuvent être transformées l'une en l'autre.

Soit une forme quadratique g réduite à la forme canonique

$$g = b_1y_1^2 + b_2y_2^2 + \ldots + b_ry_r^2, \tag{9}$$

avec $b_1, b_2, \ldots, b_r$ non nuls; elle est manifestement de rang r. Appliquant le procédé déjà utilisé ci-dessus à la réduction d'une forme du type (9) à la forme normale, il est facile de voir que l'indice d'inertie positif est égal au nombre de coefficients b_i positifs intervenant dans le second membre de l'égalité (9). De cette remarque et du théorème précédent résulte le théorème:

Une forme quadratique f est réductible à la forme canonique (9) (*par une transformation réelle non dégénérée*) *si et seulement si la forme f est de rang r et si son indice d'inertie positif est égal au nombre de coefficients b_i positifs dans le second membre de l'expression* (9).

Formes quadratiques, produits de deux formes linéaires. Multipliant deux formes linéaires de n indéterminées

$$\varphi = a_1x_1 + a_2x_2 + \ldots + a_nx_n, \quad \psi = b_1x_1 + b_2x_2 + \ldots + b_nx_n,$$

nous obtenons, manifestement, une forme quadratique. Ce n'est pas toute forme quadratique qui peut être représentée sous la forme d'un produit de deux formes linéaires; nous voulons trouver les conditions qui garantissent une telle représentation, c'est-à-dire les conditions pour lesquelles une forme quadratique peut être resprésentée comme un *produit* de deux formes linéaires.

Une forme quadratique complexe $f(x_1, x_2, \ldots, x_n)$ est le produit de deux formes linéaires si et seulement si elle est de rang deux au plus. Une forme quadratique réelle $f(x_1, x_2, \ldots, x_n)$ est le produit de deux formes linéaires si et seulement si l'une des deux conditions suivantes est vérifiée: ou bien f est de rang un au plus ou bien f est de rang deux et de signature nulle.

Considérons d'abord le produit de formes linéaires φ et ψ. Si l'une d'elles est nulle, alors leur produit est une forme quadratique à coefficients identiquement nuls et, par conséquent, de rang nul. Soient deux formes proportionnelles φ et ψ,

$$\psi = c\varphi,$$

où $c \neq 0$ et φ n'est pas identiquement nulle; on peut supposer, par exemple, que le coefficient a_1 est non nul. Alors la transformation linéaire non dégénérée

$$y_1 = a_1x_1 + \ldots + a_nx_n, \quad y_i = x_i \text{ pour } i = 2, 3, \ldots, n$$

réduit la forme quadratique $\varphi\psi$ à la forme

$$\varphi\psi = cy_1^2.$$

Le second membre est une forme quadratique de rang un, de sorte que $\varphi\psi$ a le même rang. Soient, enfin, deux formes linéaires non proportionnelles φ et ψ; on peut supposer, par exemple, que

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \neq 0.$$

Alors, la transformation linéaire

$$\begin{aligned} y_1 &= a_1x_1 + a_2x_2 + \ldots + a_nx_n, \\ y_2 &= b_1x_1 + b_2x_2 + \ldots + b_nx_n, \\ y_i &= x_i \text{ pour } i = 3, 4, \ldots, n \end{aligned}$$

est non dégénérée et réduit la forme quadratique $\varphi\psi$ à la forme

$$\varphi\psi = y_1y_2.$$

Le second membre est une forme quadratique de rang deux; de plus, dans le cas réel la signature de cette forme est nulle.

Démontrons la réciproque. Evidemment, toute forme quadratique de rang nul peut être considérée comme produit de deux formes linéaires dont l'une est identiquement nulle. Ensuite, toute forme quadratique $f(x_1, x_2, \ldots, x_n)$ de rang 1 est réductible par une transformation linéaire non dégénérée à la forme

$$f = cy_1^2, \qquad c \neq 0,$$

ou encore

$$f = (cy_1)\, y_1.$$

y_1 s'exprimant linéairement par les indéterminées $x_1, x_2, \ldots, x_n$, nous obtenons la représentation cherchée de f sous forme d'un produit de deux formes linéaires. Enfin, toute forme quadratique réelle $f(x_1, x_2, \ldots, x_n)$ de rang 2 et de signature 0 est réductible par une transformation linéaire non dégénérée à la forme

$$f = y_1^2 - y_2^2;$$

on peut réduire à la même forme toute forme quadratique complexe de rang 2. On a

$$y_1^2 - y_2^2 = (y_1 - y_2)(y_1 + y_2)$$

et, remplaçant y_1 et y_2 par leurs expressions linéaires en $x_1, x_2, \ldots, x_n$, nous obtenons le produit de deux formes linéaires en question. Le théorème est démontré.

§ 28. Formes quadratiques définies positives

Une forme quadratique f de n indéterminées à coefficients réels est dite *définie positive* si sa forme normale est la somme des carrés des indéterminées $x_1, x_2, \ldots, x_n$ avec les coefficients $+1$ ou, encore, si f est de rang n et son indice d'inertie positif est également n.

Le théorème qui suit permet de caractériser les formes quadratiques définies positives sans avoir besoin de recourir à leurs formes normales ou canoniques.

Une forme quadratique f de n indéterminées $x_1, x_2, \ldots, x_n$ à coefficients réels est définie positive si et seulement si f est positive pour toutes les valeurs réelles des indéterminées $x_1, x_2, \ldots, x_n$ telles qu'au moins une des x_i soit non nulle.

Démonstration. Supposons qu'une forme quadratique f soit réductible à la forme normale suivante:

$$f = y_1^2 + y_2^2 + \ldots + y_n^2, \tag{1}$$

par la transformation linéaire réelle

$$y_i = \sum_{j=1}^{n} a_{ij}x_j, \qquad i = 1, 2, \ldots, n, \tag{2}$$

à déterminant non nul. Si l'on veut trouver la valeur de f pour certaines valeurs réelles des x_i, on peut trouver d'abord par les formules (2) les valeurs correspondantes des y_i et, ensuite, par la formule (1), la valeur de f. Notons que si $x_1, x_2, \ldots, x_n$ ne sont pas tous nuls, alors il en est de même des $y_1, y_2, \ldots, y_n$, car, dans le cas contraire, le système d'équations linéaires homogènes à déterminant non nul

$$\sum_{j=1}^{n} a_{ij}x_j = 0, \qquad i = 1, 2, \ldots, n,$$

aurait une solution non triviale. Remplaçant dans (1) $y_1, y_2, \ldots, y_n$ par leurs valeurs (2), nous obtenons la valeur correspondante de f qui est la somme des carrés de n nombres réels non tous nuls; par conséquent, cette valeur de f sera positive.

Inversement, soit une forme f qui n'est pas définie positive; cela signifie que soit le rang, soit l'indice d'inertie positif est inférieur à n. Cela signifie encore que dans la forme normale de f (obtenue par exemple par la transformation linéaire non singulière (2)) au moins un des carrés $y_1^2, \ldots, y_n^2$, soit y_n^2, est muni du coefficient -1 ou bien du coefficient 0. Montrons qu'il existe des valeurs réelles des indéterminées $x_1, x_2, \ldots, x_n$ non toutes nulles telles que les valeurs correspondantes de f soient nulles ou même négatives. On peut trouver ces valeurs de $x_1, x_2, \ldots, x_n$ en résolvant, par exemple, au moyen de formules de Cramer, le système d'équations linéaires

obtenu de (2) avec $y_1 = y_2 = \ldots = y_{n-1} = 0$, $y_n = 1$. En effet, pour ces valeurs des indéterminées la forme f est nulle si y_n^2 n'intervient pas dans sa forme normale, et f est -1 si y_n^2 y intervient avec le coefficient -1.

Le théorème démontré joue un grand rôle dans toutes les branches où on a besoin des formes quadratiques définies positives. Néanmoins, il ne permet pas d'établir, en partant des coefficients d'une forme quadratique, si cette forme est définie positive ou non. On se sert pour cela d'un autre théorème que nous énoncerons et démontrerons lorsque nous aurons introduit une notion auxiliaire.

Soit une forme quadratique f de n indéterminées à matrice $A = (a_{ij})$. Les mineurs d'ordre k, situés à l'intersection des k premières lignes et des k premières colonnes, où $k = 1, 2, \ldots, n$, de A

$$a_{11}, \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}, \ldots, \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1k} \\ a_{21} & a_{22} & \ldots & a_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ a_{k1} & a_{k2} & \ldots & a_{kk} \end{vmatrix}, \ldots, \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}$$

sont dits *mineurs principaux* de la forme f.

Le *théorème* suivant est vrai:

Pour qu'une forme quadratique f de n indéterminées à coefficients réels soit définie positive, il faut et il suffit que tous ses mineurs principaux soient positifs.

Démonstration. Pour $n = 1$ le théorème est vrai, car, dans ce cas, la forme quadratique se réduit à un terme ax^2 et est définie positive si et seulement si $a > 0$. Aussi nous allons démontrer le théorème par récurrence sur le nombre d'indéterminées n en faisant l'hypothèse que pour $n - 1$ indéterminées le théorème soit déjà démontré.

Faisons d'abord une remarque:

Soit une forme quadratique f réelle à matrice A; toute transformation linéaire non dégénérée à matrice réelle Q conserve le *signe du déterminant de la forme f (c'est-à-dire le signe du déterminant de la matrice A).*

En effet, après une transformation linéaire à matrice Q, nous obtenons une forme quadratique dont la matrice est $Q'AQ$; or, on a $|Q'| = |Q|$, de sorte que

$$|Q'AQ| = |Q'|\cdot|A|\cdot|Q| = |A|\cdot|Q|^2,$$

c'est-à-dire le déterminant $|A|$ se trouve multiplié par un nombre positif.

Soit, maintenant, une forme quadratique

$$f = \sum_{i,\,j=1}^{n} a_{ij}x_ix_j.$$

On peut la mettre sous la forme

$$f=\varphi(x_1,\ x_2,\ \ldots,\ x_{n-1})+2\sum_{i=1}^{n-1}a_{in}x_ix_n+a_{nn}x_n^2, \tag{3}$$

où φ est une forme quadratique de $n-1$ indéterminées formée par les termes de f qui ne contiennent pas x_n. Il est clair que les mineurs principaux de la forme coïncident avec les mineurs principaux correspondants de la forme f (excepté le mineur principal d'ordre n de f).

Supposons que la forme f soit définie positive. Alors il en est de même pour la forme φ, car s'il existait des valeurs non toutes nulles de $x_1, x_2, \ldots, x_{n-1}$ qui rendaient la forme φ non positive, alors faisant $x_n = 0$, on trouverait des valeurs $x_1, x_2, \ldots, x_n$ telles que f, en vertu de (3), prenne une valeur non positive, bien que les valeurs trouvées de $x_1, x_2, \ldots, x_n$ ne soient pas toutes nulles. Ainsi, d'après l'hypothèse de récurrence, les mineurs principaux de φ sont tous positifs, de sorte que tous les mineurs principaux de f, excepté celui d'ordre n, sont tous positifs. En ce qui concerne le mineur d'ordre n de la forme f, c'est-à-dire le déterminant de la matrice A, sa positivité résulte des raisonnements suivants: la forme f étant définie positive, on peut la réduire par une transformation linéaire non dégénérée à la forme normale, c'est-à-dire à une somme de n carrés des indéterminées avec le coefficient $+1$. Le déterminant de la forme normale étant positif, il en est de même pour le déterminant de la forme f, en vertu de la remarque ci-dessus.

Supposons, à présent, que les mineurs principaux de la forme f soient tous positifs. Il en résulte que tous les mineurs principaux de la forme φ sont également positifs, de sorte que, en vertu de l'hypothèse de récurrence, φ est définie positive. Donc, il existe une transformation linéaire non dégénérée des indéterminées $x_1, x_2, \ldots$ $\ldots, x_{n-1}$ qui réduit la forme φ à la somme des carrés de $n-1$ indéterminées nouvelles, soit $y_1, y_2, \ldots, y_{n-1}$. On peut compléter cette transformation en une transformation linéaire non dégénérée de n indéterminées $x_1, x_2, \ldots, x_n$ en posant $y_n = x_n$. En vertu de (3), la forme f se réduit, par cette transformation, à la forme

$$f=\sum_{i=1}^{n-1}y_i^2+2\sum_{i=1}^{n-1}b_{in}y_iy_n+b_{nn}y_n^2; \tag{4}$$

les expressions exactes des coefficients b_{in}, par a_{ik}, n'ont aucune importance. Etant donné que

$$y_i^2+2b_{in}y_iy_n=(y_i+b_{in}y_n)^2-b_{in}^2y_n^2,$$

la transformation linéaire non dégénérée

$$\begin{aligned} z_i &= y_i+b_{in}y_n, \qquad i=1,\ 2,\ \ldots,\ n-1,\\ z_n &= \qquad y_n \end{aligned}$$

réduit, en vertu de (4), la forme f à la forme canonique

$$f=\sum_{i=1}^{n-1} z_i^2+cz_n^2. \qquad (5)$$

Pour montrer que f est définie positive, il suffit de prouver que le nombre $c>0$. Le déterminant de la forme quadratique dans le second membre de (5) est égal à c. Or, ce déterminant doit être nécessairement positif, car la forme quadratique, second membre de (5), est obtenue à partir de la forme f par deux transformations linéaires non dégénérées, et le déterminant de f, en tant que mineur principal d'ordre n de f, est positif.

Ainsi s'achève la démonstration du théorème.

Exemples. 1. La forme quadratique

$$f=5x_1^2+x_2^2+5x_3^2+4x_1x_2-8x_1x_3-4x_2x_3$$

est définie positive, car tous ses mineurs principaux sont positifs:

$$5, \quad \begin{vmatrix} 5 & 2 \\ 2 & 1 \end{vmatrix}=1, \quad \begin{vmatrix} 5 & 2 & -4 \\ 2 & 1 & -2 \\ -4 & -2 & 5 \end{vmatrix}=1.$$

2. La forme quadratique

$$f=3x_1^2+x_2^2+5x_3^2+4x_1x_2-8x_1x_3-4x_2x_3$$

n'est pas définie positive, car son mineur principal d'ordre deux est négatif

$$\begin{vmatrix} 3 & 2 \\ 2 & 1 \end{vmatrix}=-1.$$

Remarquons que, par analogie avec les formes définies positives, on peut introduire les *formes définies négatives*, c'est-à-dire les formes quadratiques réelles non dégénérées telles que leurs formes normales contiennent les carrés des indéterminées avec des coefficients -1. Les formes quadratiques dégénérées dont la forme normale contient seulement les carrés des indéterminées avec des coefficients $+1$ (ou, respectivement, -1), sont dites, quelquefois, *semi-définies*. Enfin, les formes quadratiques dont la forme normale contient les carrés des indéterminées avec des coefficients $+1$ et -1 sont dites *indéfinies*.

Chapitre VII | ESPACES VECTORIELS

§ 29. Définition d'un espace vectoriel. Isomorphisme

La définition d'un espace vectoriel à n dimensions, donnée au § 8, utilise la définition d'un vecteur, d'après laquelle un vecteur est un ensemble ordonné de n nombres. Nous avons introduit l'addition des vecteurs et la multiplication d'un vecteur par un scalaire, et cela nous a conduits à la notion d'espace vectoriel à n dimensions. Les premiers exemples d'espaces vectoriels ont été fournis par les vecteurs segments issus de l'origine des coordonnées dans un plan ou dans un espace à trois dimensions. Ayant eu à faire à ces exemples en géométrie, nous n'avons pas toujours défini les vecteurs segments par leurs coordonnées, car l'addition des vecteurs et la multiplication d'un vecteur par un scalaire peuvent être introduites du point de vue géométrique, indépendamment du choix du système des coordonnées. Notamment, on utilise la règle du parallélogramme pour définir l'addition des vecteurs, tandis que la multiplication d'un vecteur par un scalaire α signifie que ce vecteur est soumis à une homothétie de coefficient α (avec changement de sens si α est négatif). Il est logique de donner, dans le cas général, une définition d'un espace vectoriel n'utilisant pas les coordonnées, c'est-à-dire une définition qui n'exige pas la donnée d'ensembles ordonnés de nombres. Nous allons donner cette définition. Elle sera *axiomatique*. Les propriétés individuelles des vecteurs n'y jouant aucun rôle, cette définition a trait aux opérations algébriques sur les vecteurs.

Soit un ensemble V; on note les éléments de V par des lettres latines minuscules: a, b, c, ... [1]. Supposons que dans l'ensemble V soit définie une opération, dite *addition*, qui fait correspondre à tout couple d'éléments a et b de V un autre élément bien défini de V dit leur *somme* et noté $a + b$; soit une autre opération dans l'ensemble V dite *multiplication* d'un vecteur par un scalaire réel, associant à tout nombre réel α et à tout élément a de V un autre élément bien défini de V, noté αa.

---

[1] Différemment des notations adoptées au chapitre II, dans tout ce qui suit les vecteurs seront notés par des lettres latines minuscules et les nombres par des lettres grecques minuscules.

Les éléments de V sont dits *vecteurs* et l'ensemble V est appelé *espace vectoriel réel* (ou encore espace *affine* réel) si les opérations définies ci-dessus jouissent des huit propriétés suivantes:

I. L'addition est commutative: $a + b = b + a$.

II. L'addition est associative: $(a + b) + c = a + (b + c)$.

III. Il existe dans V un *élément neutre*, noté 0, vérifiant pour tout a de V l'égalité: $a + 0 = a$.

Il est facile de montrer, en s'appuyant sur la propriété I, l'*unicité de l'élément neutre*; en effet, soient deux éléments neutres 0_1 et 0_2, alors

$$0_1 + 0_2 = 0_1,$$
$$0_1 + 0_2 = 0_2 + 0_1 = 0_2,$$

d'où $0_1 = 0_2$.

IV. Pour tout élément a de V il existe dans V un *élément opposé*. noté $- a$, vérifiant l'égalité: $a + (-a) = 0$.

I et II montrent l'*unicité de l'élément opposé*; en effet, si $(-a)_1$ et $(-a)_2$ sont deux éléments opposés de a, alors

$$(-a)_1 + [a + (-a)_2] = (-a_1) + 0 = (-a)_1,$$
$$[(-a)_1 + a] + (-a)_2 = 0 + (-a)_2 = (-a)_2,$$

d'où $(-a)_1 = (-a)_2$.

On déduit des axiomes I-IV pour tout couple d'éléments a et b de V l'*existence et l'unicité de la différence* $a - b$ définie comme solution de l'équation

$$b + x = a. \tag{1}$$

En effet, posant

$$a - b = a + (-b)$$

on vérifie aisément que $a - b$ satisfait à (1):

$$b + [a + (-b)] = [b + (-b)] + a = 0 + a = a,$$

ce qui prouve l'existence de la différence. L'unicité se démontre par le raisonnement suivant: soit un autre élément c tel que (1) ait lieu, c'est-à-dire

$$b + c = a;$$

ajoutant aux deux membres de cette identité l'élément $-b$, il vient

$$c = a + (-b).$$

Les axiomes suivants (cf. § 8) établissent le lien entre l'addition et la multiplication par un scalaire, ainsi que le lien entre la multiplication par un scalaire et les opérations sur les nombres. Notamment, pour tout couple d'éléments a, b de V et pour tout couple

de nombres réels α et β les égalités suivantes doivent être vérifiées:

V. $$\alpha(a+b)=\alpha a+\alpha b;$$

VI. $$(\alpha+\beta)a=\alpha a+\beta a;$$

VII. $$(\alpha\beta)a=\alpha(\beta a);$$

VIII. $$1\cdot a=a,$$

où par le symbole 1 on a noté le nombre un.

Indiquons quelques conséquences simples de ces axiomes.

[1]. $$\alpha\cdot 0=0.$$

En effet, si a est un vecteur de V, alors on a

$$\alpha a=\alpha(a+0)=\alpha a+\alpha\cdot 0,$$

c'est-à-dire

$$\alpha\cdot 0=\alpha a-\alpha a=\alpha a+[-(\alpha a)]=0.$$

[2]. $$0\cdot a=0,$$

le symbole 0 dans le premier membre désignant le nombre réel nul et dans le second l'élément neutre de V.

En effet, si α est un nombre réel, alors

$$\alpha a=(\alpha+0)a=\alpha a+0\cdot a,$$

d'où

$$0\cdot a=\alpha a-\alpha a=0.$$

[3]. Si $\alpha a=0$, alors soit $\alpha=0$, soit $a=0$.

En effet, si $\alpha\neq 0$, c'est-à-dire si α^{-1} existe, alors

$$a=1\cdot a=(\alpha^{-1}\alpha)a=\alpha^{-1}(\alpha a)=\alpha^{-1}\cdot 0=0.$$

[4]. $$\alpha(-a)=-\alpha a.$$

En effet,

$$\alpha a+\alpha(-a)=\alpha[a+(-a)]=\alpha\cdot 0=0,$$

c'est-à-dire l'élément $\alpha(-a)$ est l'opposé de αa.

[5]. $$(-\alpha)a=-\alpha a.$$

En effet,

$$\alpha a+(-\alpha)a=[\alpha+(-\alpha)]a=0\cdot a=0,$$

c'est-à-dire l'élément $(-\alpha)a$ est l'opposé de αa.

[6]. $$\alpha(a-b)=\alpha a-\alpha b.$$

En effet, d'après [4],

$$\alpha(a-b)=\alpha[a+(-b)]=\alpha a+\alpha(-b)=\alpha a+(-\alpha b)=\alpha a-\alpha b.$$

[7]. $$(\alpha-\beta)a=\alpha a-\beta a.$$

En effet,

$$(\alpha-\beta)a=[\alpha+(-\beta)]a=\alpha a+(-\beta)a=\alpha a+(-\beta a)=\alpha a-\beta a.$$

Les axiomes I-VIII, ainsi que les propositions [1]-[7] qui en découlent, seront utilisés ultérieurement sans indications spéciales.

Nous avons donné ci-dessus la définition d'un espace vectoriel réel. Si nous avions supposé que sur l'ensemble V, outre la multiplication par les nombres réels, celle par les nombres complexes était définie, alors les mêmes axiomes I-VIII nous donneraient la notion d'*espace vectoriel complexe*. Pour fixer les idées *nous ne considérerons ci-dessous que les espaces vectoriels réels*; *néanmoins tous les résultats se rapportant aux espaces réels s'étendent au cas complexe sans aucune modification.*

Il n'y a pas de difficulté à donner des exemples d'espaces vectoriels réels. Tout d'abord, c'est l'espace vectoriel réel à n dimensions étudié au chapitre II et qui a pour éléments les vecteurs lignes. Les vecteurs segments issus de l'origine des coordonnées dans un plan ou dans un espace à trois dimensions munis de l'addition et de la multiplication par un scalaire au sens géométrique (voir le début de ce paragraphe) forment également des espaces vectoriels réels.

Il existe des exemples d'espaces vectoriels à une infinité de dimensions. Considérons les ensembles ordonnés de nombres réels qui sont de la forme

$$a=(\alpha_1,\ \alpha_2,\ \ldots,\alpha_n,\ \ldots).$$

Les opérations sur les ensembles sont appliquées aux composantes correspondantes ; notamment, si

$$b=(\beta_1,\ \beta_2,\ \ldots,\beta_n,\ \ldots),$$

alors

$$a+b=(\alpha_1+\beta_1,\ \alpha_2+\beta_2,\ \ldots,\alpha_n+\beta_n,\ \ldots);$$

d'autre part, si γ est un nombre réel, alors

$$\gamma a=(\gamma\alpha_1,\ \gamma\alpha_2,\ \ldots,\gamma\alpha_n,\ \ldots).$$

Les axiomes I-VIII sont vérifiés de sorte que nous avons dans ce cas un espace vectoriel réel.

Un autre exemple d'espace vectoriel réel à une infinité de dimensions est donné par l'ensemble des fonctions à valeurs réelles d'une variable réelle muni de l'addition et de la multiplication par les nombres réels au sens usuel de la théorie des fonctions.

Isomorphisme. A présent, nous nous proposons de trouver parmi tous les espaces vectoriels réels ceux qu'il est naturel d'appeler les espaces à un nombre fini de dimensions. D'abord introduisons une notion générale.

La définition d'un espace vectoriel utilise les propriétés des opérations sur les vecteurs et non pas les propriétés des vecteurs eux-mêmes. Cela étant, il peut arriver que les vecteurs de deux espaces vectoriels soient de nature différente, tandis que les espaces vectoriels eux-mêmes sont identiques du point de vue des propriétés des opérations algébriques définies ci-dessus. Donnons la définition exacte:

Deux espaces vectoriels réels V et V' sont dits *isomorphes* s'il existe une application bijective entre les éléments de V et V' (à tout élément a de V on associe son *image* bien définie a' dans V', deux éléments distincts de V ayant des images distinctes dans V', et inversement à tout élément a' de V' correspond son image a bien définie dans V) telle que pour tout couple d'éléments a et b de V et pour tout nombre réel α *l'image de la somme* $(a+b)$ *est la somme des images*, respectivement, de a et de b:

$$(a+b)'=a'+b', \tag{2}$$

de même que *l'image du produit* αa *est le produit du nombre* α *par l'image de* a:

$$(\alpha a)'=\alpha a'. \tag{3}$$

Notons que toute application bijective entre V et V', vérifiant les conditions (2) et (3), est dite *application isomorphe* ou *isomorphisme*.

Ainsi, l'espace des vecteurs segments issus de l'origine dans un plan est isomorphe à l'espace vectoriel à deux dimensions ayant pour éléments les couples ordonnés de nombres réels. En effet, fixant dans le plan un système de coordonnées, on obtient un isomorphisme de ces deux espaces en faisant correspondre à tout vecteur le couple ordonné de ses coordonnées.

Montrons la propriété suivante des isomorphismes d'espaces vectoriels: *soient deux espaces V et V' et une application isomorphe entre V et V'; alors l'image de l'élément neutre de V est l'élément neutre de V'.*

En effet, soient a et a' respectivement un élément de V et son image dans V'. Alors, en vertu de (2), on a

$$a'=(a+0)'=a'+0',$$

c'est-à-dire l'élément $0'$ est l'élément neutre de l'espace V'.

§ 30. Espaces à un nombre fini de dimensions. Bases

Le lecteur peut vérifier aisément que les définitions de la *dépendance linéaire* des vecteurs lignes, données au § 9, ainsi que la démonstration de leur équivalence, n'utilisent que les opérations sur les vecteurs, de sorte qu'elles peuvent être étendues au cas des espaces vectoriels. Ainsi, on peut parler des vecteurs libres, des familles maximales de vecteurs, etc., dans les espaces définis axiomatiquement.

Soient deux espaces isomorphes V et V'; pour qu'un ensemble de vecteurs $a_1, a_2, \ldots, a_k$ de V soit une famille non libre, il faut et il suffit que l'ensemble formé par leurs images $a'_1, a'_2, \ldots, a'_k$ soit une famille non libre.

Notons que si l'application $a \to a'$ est un isomorphisme, alors l'application inverse $a' \to a$ l'est également. Il suffit, donc, de considérer le cas où l'ensemble $a_1, a_2, \ldots, a_k$ est une famille non libre. Supposons qu'il existe des nombres $\alpha_1, \alpha_2, \ldots, \alpha_k$ non tous nuls tels que

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0.$$

L'image du second membre de cette égalité par l'isomorphisme considéré est l'élément neutre $0'$ de l'espace V'. Prenant l'image du premier membre par cet isomorphisme et appliquant plusieurs fois les formules (2) et (3), il vient

$$\alpha_1 a'_1 + \alpha_2 a'_2 + \ldots + \alpha_k a'_k = 0',$$

autrement dit, l'ensemble $a'_1, a'_2, \ldots, a'_k$ est une famille non libre.

Espaces à un nombre fini de dimensions. Un espace vectoriel V est dit *à un nombre fini de dimensions* si l'on peut y trouver une famille maximale formée par un nombre fini de vecteurs; s'il en est ainsi, toute famille maximale de V est dite *base* de l'espace V.

Un espace vectoriel à un nombre fini de dimensions peut avoir plusieurs bases différentes. Par exemple, dans l'espace des vecteurs segments du plan tout couple de vecteurs non colinéaires (c'est-à-dire qui ne se trouvent pas sur une même droite) forme une base de cet espace. Notons que la définition d'un espace à un nombre fini de dimensions ne donne pas la réponse à la question suivante: peut-il exister dans cet espace des bases à différents nombres de vecteurs? De plus, on pourrait même admettre l'existence de bases à un nombre arbitrairement grand de vecteurs dans un espace à un nombre fini de dimensions. Nous allons élucider quelle est la situation en réalité.

Soit dans un espace vectoriel V une base de n vecteurs

$$e_1, e_2, \ldots, e_n \tag{1}$$

Soit a un vecteur de V. La base (1) étant une famille maximale, le vecteur a est une combinaison linéaire des vecteurs (1):

$$a = \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n. \tag{2}$$

D'autre part, la famille (1) étant libre, la représentation du vecteur a sous la forme (2) est unique. En effet, admettons que

$$a = \alpha'_1 e_1 + \alpha'_2 e_2 + \ldots + \alpha'_n e_n,$$

alors

$$(\alpha_1 - \alpha'_1) e_1 + (\alpha_2 - \alpha'_2) e_2 + \ldots + (\alpha_n - \alpha'_n) e_n = 0,$$

d'où il vient

$$\alpha_i = \alpha'_i, \quad i = 1, 2, \ldots, n.$$

Ainsi, on peut associer à tout vecteur a une ligne bien définie

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \tag{3}$$

composée des coefficients de l'expression (2) de a par les vecteurs de la base (1) ou, comme nous convenons de dire, *ligne des coordonnées du vecteur a rapporté à la base* (1). Inversement, toute ligne de la forme (3), c'est-à-dire tout vecteur à n composantes, au sens du chapitre II, est la ligne des coordonnées d'un vecteur de l'espace V, rapporté à la base (1), à savoir le vecteur qui s'exprime par rapport à la base (1) sous la forme (2).

Ainsi, nous avons établi une application bijective entre les vecteurs de l'espace V et les vecteurs lignes de l'espace vectoriel à n dimensions. Montrons que cette application (qui dépend, évidemment, de la base (1)) est un isomorphisme.

Outre le vecteur a, qui dans la base (1) s'écrit sous la forme (2), prenons dans l'espace V un vecteur b qui dans la base (1) se met sous la forme

$$b = \beta_1 e_1 + \beta_2 e_2 + \ldots + \beta_n e_n.$$

On a

$$a + b = (\alpha_1 + \beta_1) e_1 + (\alpha_2 + \beta_2) e_2 + \ldots + (\alpha_n + \beta_n) e_n,$$

autrement dit, *l'espace V étant rapporté à la base* (1) *et a et b des vecteurs de V respectivement de coordonnées* (α_j) et (β_j), *la somme $a + b$ a pour coordonnées* $(\alpha_j + \beta_j)$. D'autre part,

$$\gamma a = (\gamma\alpha_1) e_1 + (\gamma\alpha_2) e_2 + \ldots + (\gamma\alpha_n) e_n,$$

c'est-à-dire *le produit γa, où γ est un scalaire et a un vecteur de V, rapporté à la base* (1), *a pour coordonnées le produit de γ par les coordonnées correspondantes de a.*

Ceci démontre le théorème:

Tout espace vectoriel, ayant une base de n éléments, est isomorphe à l'espace des vecteurs lignes à n dimensions.

On sait déjà que par isomorphisme entre deux espaces vectoriels à toute famille non libre d'un espace correspond une famille non libre d'un autre espace et inversement. Donc, toute famille libre de vecteurs conserve cette propriété après un isomorphisme quelconque. Il en résulte que l'*image de toute base d'un espace vectoriel par isomorphisme est une base du second espace.*

En effet, soient $e_1, e_2, \ldots, e_n$ une base d'un espace V et $e'_1, e'_2, \ldots, e'_n$ l'image de cette base dans l'espace V' isomorphe à V. La famille de vecteurs $e'_1, e'_2, \ldots, e'_n$ est libre. Supposons qu'elle ne soit pas maximale. Alors on peut trouver un vecteur f' de V' tel que la famille $e'_1, e'_2, \ldots, e'_n, f'$ soit encore libre. D'autre part, le vecteur f' est l'image par isomorphisme d'un vecteur f de V. Il en découle que la famille $e_1, e_2, \ldots, e_n, f$ doit être libre, ce qui est en contradiction avec la définition d'une base.

On sait également (cf. § 9) que toute famille maximale de l'espace vectoriel des lignes à n dimensions est composée de n vecteurs et que, par conséquent, toute famille de $(n + 1)$ vecteurs est non libre. En outre, toute famille libre de vecteurs est sous-famille d'une famille maximale. Tenant compte des propriétés des isomorphismes établies ci-dessus, nous sommes conduits aux résultats suivants:

Toutes les bases d'un espace vectoriel V à un nombre fini de dimensions possèdent le même nombre de vecteurs. Ce nombre étant n, l'espace V est dit *espace vectoriel à n dimensions.*

Toute famille de $(n + 1)$ vecteurs d'un espace à n dimensions est non libre.

Toute famille libre d'un espace à n dimensions appartient à une base de cet espace.

Maintenant il est facile de vérifier que les espaces vectoriels composés, respectivement, des suites infinies et des fonctions, indiqués ci-dessus, ne sont pas à un nombre fini de dimensions; en effet, le lecteur y trouvera des familles libres qui contiennent un nombre arbitrairement grand de vecteurs.

Changement de bases. Ce sont les espaces vectoriels à un nombre fini de dimensions qui font l'objet de notre étude. Evidemment, l'étude des espaces vectoriels à n dimensions se ramène à celle de l'espace vectoriel des lignes à n dimensions qui a été introduit au chapitre II. Seulement, dans le chapitre II, cet espace était rapporté à une base fixe, constituée des vecteurs e_j, dont la $j^{\text{ème}}$ coordonnée est égale à 1 et toutes les autres sont nulles, en outre, tout vecteur de l'espace rapporté à cette base était donné par la ligne de ses coordonnées; tandis que maintenant nous n'allons pas attribuer un rôle exceptionnel à une base quelconque de cet espace.

Voyons d'abord quel est le nombre de bases dans un espace vectoriel à n dimensions et quel est le rapport entre ces bases.

Soient deux bases d'un espace vectoriel V à n dimensions:

$$e_1, e_2, \ldots, e_n \tag{4}$$

et

$$e'_1, e'_2, \ldots, e'_n. \tag{5}$$

Tout vecteur de la base (5) étant un vecteur de V, il s'exprime de facon unique par les vecteurs de la base (4)

$$e'_i = \sum_{j=1}^{n} \tau_{ij} e_j, \qquad i = 1, 2, \ldots, n. \tag{6}$$

La matrice T.

$$T = \begin{pmatrix} \tau_{11} & \ldots & \tau_{1n} \\ \cdot & \cdot\ \cdot\ \cdot & \cdot \\ \tau_{n1} & \ldots & \tau_{nn} \end{pmatrix},$$

dont les lignes sont formées par les coordonnées des vecteurs (5) rapportés à la base (4), est dite *matrice de passage* de la base (4) à la base (5).

En vertu de (6), la relation entre les bases (4) et (5) et T peut être exprimée sous la forme de l'égalité matricielle:

$$\begin{pmatrix} e'_1 \\ e'_2 \\ \cdot \\ \cdot \\ e'_n \end{pmatrix} = \begin{pmatrix} \tau_{11} & \tau_{12} & \ldots & \tau_{1n} \\ \tau_{21} & \tau_{22} & \ldots & \tau_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \tau_{n1} & \tau_{n2} & \ldots & \tau_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \cdot \\ \vdots \\ e_n \end{pmatrix} \tag{7}$$

ou, désignant respectivement par e et e' les colonnes des vecteurs (4) et (5), on a encore

$$e' = Te.$$

D'autre part, notant par T' la matrice de passage de la base (5) a la base (4), on a

$$e = T'e'.$$

Il en résulte que

$$e = (T'T)\, e,$$
$$e' = (TT')\, e'$$

ou, encore, en vertu de l'indépendance linéaire des bases e et e',

$$T'T = TT' = E,$$

d'où

$$T' = T^{-1}.$$

Cela prouve que *la matrice de passage d'une base à une autre est non singulière.*

D'autre part, toute matrice carrée non singulière d'ordre n à éléments réels est une matrice de passage d'une base donnée de l'espace vectoriel à n dimensions à une autre base de cet espace.

Soient, en effet, une base (4) et une matrice non singulière T d'ordre n. La base (5) sera formée par les vecteurs qui, rapportés à la base (4), ont pour coordonnées les lignes correspondantes de la matrice T ; par conséquent, l'égalité (7) est vérifiée. La matrice T étant non singulière, le système de ses lignes et, par conséquent, la famille (5) sont libres. Donc, la famille (5), en tant que famille libre de n vecteurs, est une base de l'espace considéré et la matrice T est la matrice de passage de la base (4) à la base (5).

Ainsi, nous aboutissons au résultat suivant : dans un espace vectoriel à n dimensions on peut trouver autant de bases différentes qu'il existe de matrices carrées non singulières d'ordre n. Bien entendu, nous considérons comme distinctes les bases formées par les mêmes vecteurs, ordonnés de façon différente.

Transformation des coordonnées d'un vecteur. Soient deux bases (4) et (5) d'un espace à n dimensions et $T = (\tau_{ij})$ la matrice de passage de e à e' :

$$e' = Te.$$

Soit un vecteur a rapporté respectivement à la base (4) et à la base (5) ; il s'agit de trouver la relation qui existe entre les lignes des coordonnées de a dans ces deux bases.

Soit

$$a = \sum_{j=1}^{n} \alpha_j e_j, \tag{8}$$

$$a = \sum_{i=1}^{n} \alpha'_i e'_i.$$

Utilisant (6), il vient :

$$a = \sum_{i=1}^{n} \alpha'_i \left(\sum_{j=1}^{n} \tau_{ij} e_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \alpha'_i \tau_{ij} \right) e_j.$$

Comparant cette dernière égalité et la relation (8) on a, en vertu de l'unicité de la représentation des vecteurs par les vecteurs d'une base, la relation

$$\alpha_j = \sum_{i=1}^{n} \alpha'_i \tau_{ij}, \quad j = 1, 2, \ldots, n,$$

ou encore, sous la forme matricielle,

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\alpha'_1, \alpha'_2, \ldots, \alpha'_n)\, T.$$

Ainsi, *la ligne des coordonnées d'un vecteur a, rapporté à la base e, est égale à la ligne des coordonnées de a, rapporté à la base e', multipliée à droite par la matrice de passage T.*

Bien entendu, il en résulte l'égalité

$$(\alpha'_1, \alpha'_2, \ldots, \alpha'_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)\, T^{-1}.$$

Exemple. Considérons l'espace à trois dimensions ayant pour base les vecteurs

$$e_1,\ e_2,\ e_3. \tag{9}$$

Les vecteurs

$$\left.\begin{aligned} e'_1 &= 5e_1 - e_2 - 2e_3, \\ e'_2 &= 2e_1 + 3e_2, \\ e'_3 &= -2e_1 + e_2 + e_3 \end{aligned}\right\} \tag{10}$$

forment une autre base de cet espace, la matrice de passage de la base (9) à la base (10) étant de la forme

$$T = \begin{pmatrix} 5 & -1 & -2 \\ 2 & 3 & 0 \\ -2 & 1 & 1 \end{pmatrix};$$

on a

$$T^{-1} = \begin{pmatrix} 3 & -1 & 6 \\ -2 & 1 & -4 \\ 8 & -3 & 17 \end{pmatrix}$$

Ainsi, le vecteur

$$a = e_1 + 4e_2 - e_3,$$

rapporté à la base (10), a pour ligne des coordonnées la ligne

$$(\alpha'_1, \alpha'_2, \alpha'_3) = (1, 4, -1) \begin{pmatrix} 3 & -1 & 6 \\ -2 & 1 & -4 \\ 8 & -3 & 17 \end{pmatrix} = (-13, 6, -27),$$

c'est-à-dire

$$a = -13e'_1 + 6e'_2 - 27e'_3.$$

§ 31. Applications linéaires

Nous avons déjà rencontré au chapitre III la notion de transformation linéaire des indéterminées. La notion que nous allons introduire maintenant est d'un autre caractère. D'ailleurs, il n'y aurait aucune difficulté d'établir le lien qui existe entre ces deux notions.

Soit un espace vectoriel réel à n dimensions, noté V_n. Considérons une transformation de cet espace dans lui-même, c'est-à-dire

une application qui associe à *tout* vecteur a de V_n un vecteur a' de cet espace. Le vecteur a' est appelé *image* du vecteur a par l'application considérée.

Désignant par φ l'application en question, on convient de noter $a\varphi$ l'image du vecteur a par l'application φ (et non pas $\varphi(a)$ ou encore φa) ; on a

$$a' = a\varphi.$$

La transformation φ d'un espace vectoriel V_n est appelée *application linéaire* de V_n si la somme de tout couple de vecteurs a, b de V_n a pour image la somme des images de a et de b:

$$(a+b)\varphi = a\varphi + b\varphi, \tag{1}$$

et si le produit de tout vecteur a de V_n par un scalaire réel α a pour image le produit de α par l'image de a:

$$(\alpha a)\varphi = \alpha(a\varphi). \tag{2}$$

Il résulte immédiatement de cette définition que *toute application linéaire d'un espace vectoriel associe à une combinaison linéaire des vecteurs a_1, a_2, . . ., a_k la combinaison linéaire de leurs images avec les mêmes coefficients*:

$$(\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k)\varphi = \alpha_1(a_1\varphi) + \alpha_2(a_2\varphi) + \ldots + \alpha_k(a_k\varphi). \tag{3}$$

Démontrons la proposition suivante :

Toute application linéaire φ d'un espace vectoriel V_n conserve le vecteur nul,

$$0\varphi = 0,$$

et pour tout vecteur a de V_n l'image de $-a$ par φ est le vecteur $-a\varphi$:

$$(-a)\varphi = -a\varphi.$$

En effet, tenant compte de (2), on a pour tout vecteur b de V_n

$$0\varphi = (0 \cdot b)\varphi = 0 \cdot (b\varphi) = 0.$$

D'autre part,

$$(-a)\varphi = [(-1)a]\varphi = (-1)(a\varphi) = -a\varphi.$$

La notion d'application linéaire d'un espace vectoriel dans lui-même est une généralisation de celle de transformation affine d'un plan ou d'un espace à trois dimensions connue du cours de géométrie analytique; de fait, les conditions (1) et (2) sont toujours vérifiées pour les transformations affines. Ces conditions sont encore vraies pour les projections des vecteurs d'un plan ou d'un espace à trois dimensions sur une droite (ou sur un plan). Par exemple, la transformation de l'espace vectoriel à deux dimensions, ayant

pour éléments les vecteurs segments issus de l'origine, qui associe à tout vecteur sa projection sur un axe passant par l'origine, est une application linéaire.

L'*application identique* ε donnée dans un espace vectoriel V_n, qui conserve tout vecteur a de V_n:

$$a\varepsilon = a,$$

ainsi que l'*application nulle* ω, qui fait correspondre à tout vecteur a de V_n le vecteur nul,

$$a\omega = 0,$$

sont des exemples d'applications linéaires.

Maintenant, nous passons à la description des applications linéaires d'un espace vectoriel V_n. Soit une base de V_n:

$$e_1,\ e_2,\ \ldots,\ e_n; \tag{4}$$

exactement comme ci-dessus, la base (4), rangée en une colonne, est notée par e. Tout vecteur a de V_n étant une combinaison linéaire bien définie des vecteurs (4), l'image de a est, en vertu de (3), la combinaison linéaire avec les mêmes coefficients des images des vecteurs e_j. En d'autres termes, *toute application linéaire* φ *de* V_n *est bien définie par les images* $e_1\varphi$, $e_2\varphi$, ..., $e_n\varphi$ *des vecteurs d'une base fixe quelconque de l'espace vectoriel* V_n.

Quelle que soit la famille ordonnée de n *vecteurs de* V_n,

$$c_1,\ c_2,\ \ldots,\ c_n, \tag{5}$$

il existe une application linéaire unique dans V_n *telle que les vecteurs* c_1, c_2, ..., c_n *de la famille* (5) *soient respectivement les images des vecteurs* e_1, e_2, ..., e_n *de la base* (4) *par l'application*

$$e_i\varphi = c_i, \qquad i = 1, 2, \ldots, n. \tag{6}$$

L'unicité de l'application φ ayant été montrée ci-dessus, il suffit de démontrer son existence. Définissons l'application φ de la manière suivante: si a est un vecteur quelconque de V_n, qui, rapporté à la base (4), est de la forme

$$a = \sum_{i=1}^{n} \alpha_i e_i,$$

nous définissons l'application φ par l'égalité

$$a\varphi = \sum_{i=1}^{n} \alpha_i c_i. \tag{7}$$

Montrons que, ainsi définie, l'application φ est linéaire. En effet, soit un autre vecteur b de V_n, qui, rapporté à la base (4), s'expri-

me par la combinaison linéaire

$$b = \sum_{i=1}^{n} \beta_i e_i.$$

Alors, on a

$$(a+b)\varphi = [\sum_{i=1}^{n} (\alpha_i + \beta_i) e_i]\varphi =$$
$$= \sum_{i=1}^{n} (\alpha_i + \beta_i) c_i = \sum_{i=1}^{n} \alpha_i c_i + \sum_{i=1}^{n} \beta_i c_i = a\varphi + b\varphi.$$

D'autre part, γ étant un scalaire réel, il vient:

$$(\gamma a)\varphi = [\sum_{i=1}^{n} (\gamma\alpha_i) e_i]\varphi = \sum_{i=1}^{n} (\gamma\alpha_i) c_i =$$
$$= \gamma \sum_{i=1}^{n} \alpha_i c_i = \gamma (a\varphi).$$

En outre, les relations (6) sont vérifiées car elles résultent de la définition même (7) de l'application φ; en effet, la $i^{\text{ème}}$ coordonnée du vecteur e_i, rapporté à la base (4), est égale à l'unité et toutes les autres coordonnées sont nulles.

Ainsi, nous avons une application bijective entre les applications linéaires d'un espace vectoriel V_n et les familles ordonnées de n vecteurs (5) *de cet espace.*

Or, tout vecteur c_i, rapporté à la base (4), a des coordonnées bien définies, de sorte que l'on a les égalités

$$c_i = \sum_{j=1}^{n} \alpha_{ij} e_j, \qquad i = 1, 2, \ldots, n, \tag{8}$$

avec α_{ij} bien définis. Les coordonnées du vecteur c_i, rapporté à la base (4), forment une matrice carrée d'ordre n,

$$A = (\alpha_{ij}), \tag{9}$$

qui a pour sa $i^{\text{ème}}$ ligne celle des coordonnées du vecteur c_i (avec $1 \leqslant i \leqslant n$). La famille (5) ayant été choisie arbitrairement, la matrice A d'ordre n est quelconque, mais à éléments réels.

Ainsi, nous avons une application bijective entre les applications linéaires données dans un espace vectoriel V_n et les matrices carrées d'ordre n; bien entendu, cette application dépend du choix de la base (4).

La base (4) étant fixe, nous dirons que la matrice A *donne* une application linéaire φ ou, encore, que A est la *matrice de l'application* φ, rapportée à la base (4). Notant $e\varphi$ la colonne des images des

vecteurs de la base (4) et comparant les relations (6), (8) et (9). on en déduit l'égalité matricielle

$$e\varphi = Ae \tag{10}$$

qui décrit entièrement la relation qui existe entre une application linéaire φ, une base e et la matrice A de l'application φ, rapportée à la base e. φ étant une application linéaire qui, rapportée à la base (4), a A pour matrice, a étant un vecteur quelconque, il s'agit de trouver, en partant des coordonnées de a, rapporté à la base (4). les coordonnées de $a\varphi$ rapporté à la même base. Si

$$a = \sum_{i=1}^{n} \alpha_i e_i,$$

alors,

$$a\varphi = \sum_{i=1}^{n} \alpha_i (e_i\varphi),$$

la dernière relation est équivalente à l'égalité matricielle

$$a\varphi = (\alpha_1, \alpha_2, \ldots, \alpha_n)(e\varphi).$$

Compte tenu de (10) et de l'associativité de la multiplication des matrices (cette dernière se vérifie aisément dans le cas où l'un des facteurs est une colonne de vecteurs), on obtient:

$$a\varphi = [(\alpha_1, \alpha_2, \ldots, \alpha_n) A] e.$$

Il en résulte que *la ligne des coordonnées du vecteur* $a\varphi$ *est le produit à droite de la ligne des coordonnées du vecteur* a *par la matrice* A *de l'application linéaire* φ *(*$a\varphi$*,* a *et* φ *étant rapportés à la base* (4)).

Exemple. Soient un espace vectoriel à trois dimensions et une application linéaire φ, qui, rapportée à une base e_1, e_2, e_3, a pour matrice

$$A = \begin{pmatrix} -2 & 1 & 0 \\ 1 & 3 & 2 \\ 0 & -4 & 1 \end{pmatrix}$$

Si

$$a = 5e_1 + e_2 - 2e_3,$$

alors

$$(5, 1, -2) \begin{pmatrix} -2 & 1 & 0 \\ 1 & 3 & 2 \\ 0 & -4 & 1 \end{pmatrix} = (-9, 16, 0),$$

c'est-à-dire

$$a\varphi = -9e_1 + 16e_2.$$

Changement de bases et relation entre les matrices correspondantes d'une application linéaire. Bien entendu, la matrice d'une application linéaire dépend de la base, à laquelle cette application est

rapportée. Etablissons la relation qui existe entre les matrices d'une application linéaire rapportée à des bases différentes.

Soient deux bases e et e' et la matrice de passage T de e à e' :

$$e' = Te. \tag{11}$$

Soient A et A' les matrices d'une application linéaire φ rapportée respectivement aux bases e et e', de sorte que

$$e\varphi = Ae, \qquad e'\varphi = A'e'. \tag{12}$$

Compte tenu de (11), la seconde égalité (12) donne

$$(Te)\,\varphi = A'\,(Te).$$

Or,

$$(Te)\,\varphi = T\,(e\varphi).$$

En effet, si $(\tau_{i1}, \tau_{i2}, \ldots, \tau_{in})$ est la $i^{\text{ème}}$ ligne de la matrice T, alors

$$(\tau_{i1}e_1 + \tau_{i2}e_2 + \ldots + \tau_{in}e_n)\,\varphi = \tau_{i1}\,(e_1\varphi) + \\ + \tau_{i2}\,(e_2\varphi) + \ldots + \tau_{in}\,(e_n\varphi).$$

Ainsi, en vertu des relations (12), on a

$$(Te)\,\varphi = T\,(e\varphi) = T\,(Ae) = (TA)\,e,$$
$$A'\,(Te) = (A'T)\,e$$

ou encore

$$(TA)\,e = (A'T)\,e.$$

Si au moins pour un i (avec $1 \leqslant i \leqslant n$), la $i^{\text{ème}}$ ligne de la matrice TA était différente de la $i^{\text{ème}}$ ligne de la matrice $A'T$, cela signifierait que deux combinaisons linéaires différentes des vecteurs $e_1, e_2, \ldots, e_n$ coïncident, ce qui est en contradiction avec l'indépendance linéaire des vecteurs de la base e. Ainsi, on a

$$TA = A'T,$$

d'où, en vertu de la non-singularité de la matrice de passage T, on obtient les relations

$$A' = TAT^{-1}, \qquad A = T^{-1}A'T. \tag{13}$$

Deux matrices carrées B et C telles que l'on ait l'égalité

$$C = Q^{-1}BQ,$$

où Q est une matrice carrée non singulière, sont dites *matrices semblables*. En outre, on dira que la matrice C est la transmuée (ou, encore, transformée) de la matrice B par la matrice Q.

Les égalités (13), établies ci-dessus, peuvent être ainsi énoncées sous la forme d'un théorème.

Les matrices d'une même application linéaire, rapportée à des bases différentes, sont toutes semblables. En outre, la matrice d'une application linéaire φ *rapportée à une base* e' *s'obtient en transmuant la matrice de* φ *rapportée à une base* e *par la matrice de passage de* e' *à* e.

Il faut souligner que si une application linéaire φ rapportée à une base e a A pour matrice, alors toute matrice B semblable à A, c'est-à-dire telle que

$$B = Q^{-1}AQ,$$

est la matrice de l'application φ rapportée à une autre base, à savoir à celle qui s'obtient de e par la matrice de passage Q^{-1}.

Opérations sur les applications linéaires. Fixant une base dans l'espace V_n et faisant correspondre à toute application linéaire donnée dans V_n la matrice de cette application rapportée à la base fixe, on obtient, comme il a été démontré ci-dessus, une application bijective entre les applications linéaires et les matrices carrées d'ordre n. Il est naturel de s'attendre à ce que l'addition et la multiplication des matrices, ainsi que la multiplication d'une matrice par un scalaire, se traduisent par les mêmes opérations sur les applications linéaires correspondantes.

Soient deux applications linéaires φ et ψ données dans un espace vectoriel V_n. L'application $\varphi + \psi$, définie par l'égalité

$$a(\varphi + \psi) = a\varphi + a\psi, \tag{14}$$

est dite *somme* de φ et ψ ; elle associe donc à tout vecteur a de V_n la somme des images de a, respectivement par les applications φ et ψ.

L'application $\varphi + \psi$ *est linéaire.* En effet, pour tout couple de vecteurs a et b de V_n et pour tout scalaire α, on a

$$(a + b)(\varphi + \psi) = (a + b)\varphi + (a + b)\psi =$$
$$= a\varphi + b\varphi + a\psi + b\psi = a(\varphi + \psi) + b(\varphi + \psi);$$
$$(\alpha a)(\varphi + \psi) = (\alpha a)\varphi + (\alpha a)\psi = \alpha(a\varphi) + \alpha(a\psi) =$$
$$= \alpha(a\varphi + a\psi) = \alpha[a(\varphi + \psi)].$$

D'autre part, on appelle *produit* de deux applications linéaires φ et ψ une application $\varphi\psi$ telle que l'on ait pour tout vecteur a de V_n :

$$a(\varphi\psi) = (a\varphi)\psi; \tag{15}$$

autrement dit $\varphi\psi$ est le résultat de l'application successive de φ et de ψ.

L'application $\varphi\psi$ *est linéaire* ; en effet,

$$(a + b)(\varphi\psi) = [(a + b)\varphi]\psi = (a\varphi + b\varphi)\psi =$$
$$= (a\varphi)\psi + (b\varphi)\psi = a(\varphi\psi) + b(\varphi\psi);$$
$$(\alpha a)(\varphi\psi) = [(\alpha a)\varphi]\psi =$$
$$= [\alpha(a\varphi)]\psi = \alpha[(a\varphi)\psi] = \alpha[a(\varphi\psi)].$$

Enfin, $\varkappa$ étant un scalaire et φ une application linéaire, on appelle *produit de* φ *par* $\varkappa$ une application $\varkappa\varphi$ telle que l'on ait

$$a(\varkappa\varphi) = \varkappa(a\varphi); \tag{16}$$

l'image d'un vecteur par l'application $\varkappa\varphi$ est, donc, le produit du scalaire $\varkappa$ et de l'image de ce vecteur par l'application φ.

L'application $\varkappa\varphi$ *est linéaire*; en effet,

$$\begin{aligned}(a+b)(\varkappa\varphi) &= \varkappa[(a+b)\varphi] = \varkappa(a\varphi + b\varphi) = \\ &= \varkappa(a\varphi) + \varkappa(b\varphi) = a(\varkappa\varphi) + b(\varkappa\varphi); \\ (\alpha a)(\varkappa\varphi) &= \varkappa[(\alpha a)\varphi] = \varkappa[\alpha(a\varphi)] = \\ &= \alpha[\varkappa(a\varphi)] = \alpha[a(\varkappa\varphi)].\end{aligned}$$

Supposons que les applications linéaires φ et ψ, rapportées toutes deux à une base $e_1, e_2, \ldots, e_n$, ont pour matrices correspondantes respectivement A et B, $A = (\alpha_{ij})$, $B = (\beta_{ij})$:

$$e\varphi = Ae, \quad e\psi = Be.$$

Alors, en vertu de (14), on a

$$\begin{aligned}e_i(\varphi + \psi) = e_i\varphi + e_i\psi &= \sum_{j=1}^{n} \alpha_{ij}e_j + \sum_{j=1}^{n} \beta_{ij}e_j = \\ &= \sum_{j=1}^{n} (\alpha_{ij} + \beta_{ij})\, e_j,\end{aligned}$$

ou encore

$$e(\varphi + \psi) = (A + B)\, e.$$

Ainsi, la matrice de la somme d'applications linéaires rapportée à une base est égale à la somme des matrices de ces applications rapportées à la même base.

D'autre part, compte tenu de (15), on a

$$\begin{aligned}e_i(\varphi\psi) = (e_i\varphi)\,\psi = \Big(\sum_{j=1}^{n} \alpha_{ij}e_j\Big)\,\psi &= \sum_{j=1}^{n} \alpha_{ij}(e_j\psi) = \\ = \sum_{j=1}^{n} \alpha_{ij}\Big(\sum_{k=1}^{n} \beta_{jk}e_k\Big) &= \sum_{k=1}^{n}\Big(\sum_{j=1}^{n} \alpha_{ij}\beta_{jk}\Big)\, e_k,\end{aligned}$$

ou encore

$$e(\varphi\psi) = (AB)\, e.$$

Autrement dit, *la matrice du produit de deux applications linéaires rapporté à une base est le produit des matrices de ces applications rapportées à la même base.*

Enfin, en vertu de (16), on a

$$e_i(\varkappa\varphi)=\varkappa\,(e_i\varphi)=\varkappa\sum_{j=1}^{n}\alpha_{ij}e_j=\sum_{j=1}^{n}(\varkappa\alpha_{ij})\,e_j,$$

ou encore

$$e\,(\varkappa\varphi)=(\varkappa A)\,e.$$

Par conséquent, *la matrice de l'application* $\varkappa\varphi$ *(où* $\varkappa$ *est un scalaire et* φ *une application linéaire) rapportée à une base est le produit de* $\varkappa$ *par la matrice de l'application* φ *rapportée à cette même base.*

Il s'ensuit que les opérations sur les applications linéaires jouissent des mêmes propriétés que les opérations correspondantes sur les matrices. Ainsi, l'addition des applications linéaires est commutative et associative, tandis que leur multiplication est associative et non commutative pour $n>1$. La différence des applications linéaires est également bien définie. Il faut souligner que *l'application identique* ε *joue le rôle de l'élément unité dans l'ensemble des applications linéaires, tandis que le rôle de l'élément nul est tenu par l'application linéaire nulle* ω. En effet, les applications linéaires ε et ω rapportées à une base quelconque ont pour matrices respectivement la matrice unité et la matrice nulle.

§ 32*. Sous-espaces d'un espace vectoriel

Un sous-ensemble L d'un espace vectoriel V est appelé *sous-espace vectoriel* de V si L est un espace vectoriel par rapport à l'addition des vecteurs et à la multiplication d'un vecteur par un scalaire définies dans V. Ainsi, dans un espace euclidien à trois dimensions l'ensemble des vecteurs issus de l'origine et appartenant à un plan (ou à une droite), passant par l'origine, forme un sous-espace vectoriel.

Pour qu'un sous-ensemble L *non vide soit un sous-espace vectoriel d'un espace vectoriel* V, *il suffit que les conditions suivantes soient vérifiées:*

1. *Si les vecteurs* a *et* b *appartiennent à* L, *alors* L *contient également le vecteur* $a+b$.

2. *Si le vecteur* a *appartient à* L, *alors* αa *appartient également à* L *quel que soit le scalaire* α.

En effet, en vertu de la condition 2, L contient le vecteur nul, car si a appartient à L, alors $0\cdot a=0$ appartient également à L. Ensuite, si le vecteur a appartient à L, alors son opposé $-a$ est également un élément de L, compte tenu de la condition 2 et de l'égalité $-a=(-1)\cdot a$. Ceci entraîne, en vertu de la condition 1, que la différence des deux vecteurs de L appartient encore à L. Les autres conditions de la définition d'un espace vectoriel étant valables pour V, elles sont, en particulier, vérifiées pour L.

L'espace vectoriel V ainsi que l'ensemble composé de l'élément nul de V nous fournissent deux exemples de sous-espaces vectoriels de V (le second est dit *sous-espace nul*). Un exemple moins banal s'obtient par le procédé suivant : soit

$$a_1, a_2, \ldots, a_r \tag{1}$$

une famille finie quelconque de vecteurs de V et soit L l'ensemble de toutes les combinaisons linéaires des vecteurs de la famille (1). Montrons que L est un sous-espace vectoriel. En effet, si

$$b = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_r a_r, \quad c = \beta_1 a_1 + \beta_2 a_2 + \ldots + \beta_r a_r,$$

alors

$$b + c = (\alpha_1 + \beta_1) a_1 + (\alpha_2 + \beta_2) a_2 + \ldots + (\alpha_r + \beta_r) a_r,$$

c'est-à-dire le vecteur $b + c$ appartient à L ; de même, si b est un élément de L, alors le vecteur

$$\gamma b = (\gamma\alpha_1) a_1 + (\gamma\alpha_2) a_2 + \ldots + (\gamma\alpha_r) a_r$$

appartient également à L, quel que soit le nombre γ.

Le sous-espace L est dit *engendré* par la famille de vecteurs (1) ; L contient, en particulier, tout vecteur de la famille (1).

D'ailleurs, *tout sous-espace vectoriel à un nombre fini de dimensions est engendré par une famille finie de vecteurs*, car il possède une base finie (excepté le cas où le sous-espace est nul). La dimension d'un sous-espace vectoriel L ne dépasse pas celle de l'espace V_n ; en outre, la dimension de L est égale à n si et seulement si $L = V_n$. Bien entendu, nous conviendrons que la dimension du sous-espace vectoriel nul est le nombre 0.

Pour tout entier k (avec $0 < k < n$), il existe dans l'espace V_n un sous-espace vectoriel de dimension k. Pour montrer cela, il suffit de prendre le sous-espace vectoriel de V_n engendré par une famille libre de k vecteurs de V_n.

Soient deux sous-espaces vectoriels L_1 et L_2 d'un espace V. L'ensemble des vecteurs appartenant simultanément à L_1 et à L_2 est encore un sous-espace vectoriel noté L_0 ; cela se vérifie facilement. Le sous-espace vectoriel L_0 est l'*intersection* de L_1 et L_2. D'autre part, l'ensemble des vecteurs de la forme $a + b$, où a appartient à L_1 et b à L_2, est encore un sous-espace vectoriel noté $\overline{L}$; $\overline{L}$ est la *somme* de L_1 et L_2. Désignant les dimensions de L_1, L_2, L_0 et $\overline{L}$ respectivement par d_1, d_2, d_0 et $\overline{d}$, on a la formule :

$$\overline{d} = d_1 + d_2 - d_0, \tag{2}$$

autrement dit, la *dimension de la somme de deux sous-espaces vectoriels est la somme des dimensions de ces sous-espaces de laquelle on retranche la dimension de leur intersection.*

14—1212

Pour démontrer cette formule, fixons une base quelconque de L_0

$$a_1,\ a_2,\ \ldots,\ a_{d_0}; \tag{3}$$

complétons la famille (3) par les vecteurs $b_{d_0+1}, \ldots, b_{d_1}$ en une base sur L_1, soit

$$a_1,\ a_2,\ \ldots,\ a_{d_0},\ b_{d_0+1},\ \ldots,\ b_{d_1}, \tag{4}$$

et par les vecteurs $c_{d_0+1}, \ldots, c_{d_2}$ en une base sur L_2, soit

$$a_1,\ a_2,\ \ldots,\ a_{d_0},\ c_{d_0+1},\ \ldots,\ c_{d_2}. \tag{5}$$

Utilisant la définition du sous-espace vectoriel $\overline{L}$, on vérifie aisément que $\overline{L}$ est engendré par la famille des vecteurs

$$a_1,\ a_2,\ \ldots,\ a_{d_0},\ b_{d_0+1},\ \ldots,\ b_{d_1},\ c_{d_0+1},\ \ldots,\ c_{d_2}. \tag{6}$$

La formule (2) sera donc démontrée si nous démontrons que les vecteurs (6) forment une famille libre.

Supposons le contraire, c'est-à-dire que l'on ait :

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_{d_0} a_{d_0} + \beta_{d_0+1} b_{d_0+1} + \ldots + \\ + \beta_{d_1} b_{d_1} + \gamma_{d_0+1} c_{d_0+1} + \ldots + \gamma_{d_2} c_{d_2} = 0$$

avec certains coefficients numériques. Alors

$$d = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_{d_0} a_{d_0} + \beta_{d_0+1} b_{d_0+1} + \ldots \\ \ldots + \beta_{d_1} b_{d_1} = -\gamma_{d_0+1} c_{d_0+1} - \ldots - \gamma_{d_2} c_{d_2}. \tag{7}$$

Le premier membre de (7) appartient à L_1, le second est un élément de L_2, de sorte que le vecteur d, valeur commune des deux membres, appartient à L_0 et s'exprime donc par les vecteurs de la base (3). Or, le second membre de (7) montre que le vecteur d s'exprime également par les vecteurs $c_{d_0+1}, \ldots, c_{d_2}$. Il en résulte, compte tenu de l'indépendance linéaire des vecteurs (5), que tous les coefficients $\gamma_{d_0+1}, \ldots, \gamma_{d_2}$ sont nuls et, par conséquent, $d = 0$. Or, la famille (4) étant libre, on déduit de l'égalité $d = 0$ que tous les coefficients $\alpha_1, \ldots, \alpha_{d_0}, \beta_{d_0+1}, \ldots, \beta_{d_1}$ sont également nuls. Ceci achève la démonstration de l'indépendance linéaire des vecteurs (6).

On laisse au lecteur le soin de vérifier que notre démonstration est encore valable dans le cas où L_0 est un sous-espace vectoriel nul, c'est-à-dire où $d_0 = 0$.

Image et noyau d'une application linéaire. Soit une application linéaire φ d'un espace vectoriel V_n dans lui-même. Les définitions d'un sous-espace vectoriel et d'une application linéaire entraînent immédiatement que pour tout sous-espace vectoriel L de V_n *l'ensemble $L\varphi$ des images des vecteurs de L par l'application φ est encore un sous-espace vectoriel.* En particulier, l'ensemble $V_n\varphi$ des images

des vecteurs de V_n par l'application φ est un sous-espace vectoriel, dit *image de l'application* φ.

Calculons la dimension de l'image de φ. Pour cela, rappelons que les matrices d'une application linéaire φ rapportée à des bases différentes sont toutes semblables et, en vertu du dernier théorème du § 14, ont toutes le même rang. On peut donc appeler ce nombre *rang* de l'application linéaire φ.

La dimension de l'image d'une application linéaire φ *est égale au rang de* φ.

En effet, soit A la matrice de φ rapportée à une base $e_1, e_2, \ldots$ $\ldots, e_n$. Le sous-espace vectoriel $V_n\varphi$ est engendré par les vecteurs

$$e_1\varphi, e_2\varphi, \ldots, e_n\varphi \tag{8}$$

de sorte que toute sous-famille maximale de la famille (8) peut être choisie comme base du sous-espace $V_n\varphi$. Or, le nombre maximal de vecteurs linéairement indépendants de la famille (8) est égal au nombre maximal de lignes linéairement indépendantes de la matrice A ; autrement dit, il est égal au rang de A. Ceci achève la démonstration du théorème.

On sait que l'image du vecteur nul par toute application linéaire φ est le vecteur nul. Ainsi, l'ensemble $N(\varphi)$ des vecteurs de V_n, dont les images par l'application φ sont le vecteur nul, est non vide ; en outre, il est clair que $N(\varphi)$ est un sous-espace vectoriel. $N(\varphi)$ est appelé *noyau* de l'application linéaire φ, tandis que la dimension de $N(\varphi)$ est appelée *dimension du noyau* ou, encore, *déficit* de φ.

Quelle que soit l'application linéaire φ *de l'espace vectoriel* V_n *dans lui-même, la somme du rang et de la dimension du noyau de* φ (ou codimension de l'image de V_n par l'application φ) *est égale à la dimension* n *de l'espace* V_n.

En effet, soit r le rang de φ ; alors le sous-espace vectoriel $V_n\varphi$ possède une base de r vecteurs

$$a_1, a_2, \ldots, a_r. \tag{9}$$

On peut trouver dans V_n des vecteurs

$$b_1, b_2, \ldots, b_r \tag{10}$$

tels que

$$b_i\varphi = a_i, \qquad i = 1, 2, \ldots, r;$$

évidemment, les vecteurs (10) en général ne sont pas définis de façon unique. S'il existait une combinaison linéaire non triviale des vecteurs (10) telle que l'image de cette combinaison par l'application φ soit le vecteur 0 (et, en particulier, si les vecteurs (10) étaient linéairement dépendants), alors les vecteurs (9) seraient linéairement

dépendants, contrairement à leur choix. Il en résulte que le sous-espace vectoriel L engendré par les vecteurs (10) est à r dimensions et a le vecteur nul pour unique élément commun avec $N(\varphi)$.

D'autre part, la somme des sous-espaces vectoriels L et $N(\varphi)$ est l'espace V_n. En effet, soit c un vecteur de V_n; il est clair que le vecteur $d = c\varphi$ appartient au sous-espace $V_n\varphi$. On peut, donc, trouver un vecteur b de L tel que

$$b\varphi = d$$

(pour trouver b, il suffit de remarquer que les coordonnées du vecteur b rapporté à la base (10) coïncident avec les coordonnées du vecteur d rapporté à la base (9)). Il résulte de cette dernière égalité et de la définition du vecteur d que le vecteur $c - b$ appartient au sous-espace $N(\varphi)$, car

$$(c-b)\varphi = c\varphi - b\varphi = d - d = 0.$$

Ainsi,

$$c = b + (c-b)$$

avec $(c - b)$ appartenant à $N(\varphi)$.

Les résultats obtenus et la formule (2) démontrée ci-dessus achèvent la démonstration du théorème.

Applications linéaires non dégénérées. Une application linéaire φ de l'espace vectoriel V_n dans lui-même est dite *non dégénérée* (ou non singulière) si elle vérifie l'une des conditions suivantes (l'équivalence de ces conditions résulte immédiatement des théorèmes démontrés ci-dessus):

1. *L'application φ est de rang n.*
2. *L'image de l'application φ coïncide avec V_n.*
3. *L'application φ est telle que son noyau est de dimension nulle.*

On peut donner d'autres définitions équivalentes. Par exemple.

4. *Pour tout couple de vecteurs a et b de V_n, $a \neq b$, leurs images par l'application linéaire φ vérifient l'inégalité $a\varphi \neq b\varphi$.*

En effet, si l'application φ satisfait à la condition 4, alors le noyau de φ se réduit à l'élément nul, de sorte que la condition 3 est également vérifiée. Si, d'autre part, il existe des vecteurs a et b de V_n tels que $a \neq b$ et $a\varphi = b\varphi$, c'est-à-dire tels que $a - b \neq 0$ et $(a - b)\varphi = 0$, cela signifie que la condition 3 n'est pas satisfaite.

2 et 4 entraînent:

5. *Une application linéaire φ est une application bijective de l'espace vectoriel V_n sur lui-même.*

De la condition 5 résulte l'existence de l'*application inverse* φ^{-1} pour toute application linéaire φ non dégénérée: φ^{-1} associe à tout vecteur $a\varphi$ le vecteur a:

$$(a\varphi)\varphi^{-1} = a.$$

L'application φ^{-1} *est linéaire*, car

$$(a\varphi + b\varphi)\varphi^{-1} = [(a+b)\varphi]\varphi^{-1} = a+b,$$
$$[\alpha(a\varphi)]\varphi^{-1} = [(\alpha a)\varphi]\varphi^{-1} = \alpha a.$$

La définition de l'application φ^{-1} entraîne les égalités

$$\varphi\varphi^{-1} = \varphi^{-1}\varphi = \varepsilon, \tag{11}$$

qui peuvent être considérées comme définition de l'application inverse. Il s'ensuit de (11) et des résultats obtenus à la fin du paragraphe précédent la proposition suivante: *soit A la matrice d'une application linéaire non dégénérée* φ *rapportée à une base* (*A est*, *en vertu de la condition* 1, *non dégénérée*); *alors*, *l'application* φ^{-1}, *rapportée à la même base*, *a* A^{-1} *pour matrice*.

Nous sommes donc conduits à la définition suivante d'une application linéaire non dégénérée:

6. *L'application* φ *est non dégénérée si l'application linéaire inverse* φ^{-1} *existe*.

§ 33. Racines caractéristiques et valeurs propres

Soit $A = (\alpha_{ij})$ une matrice carrée d'ordre n à éléments réels. La matrice $A - \lambda E$, où λ est une inconnue et E matrice unité d'ordre n, est appelée *matrice caractéristique* de A. Etant donné que la matrice λE a λ pour éléments de sa diagonale principale et que tous les autres éléments de λE sont nuls, la matrice $A - \lambda E$ est de la forme

$$A - \lambda E = \begin{pmatrix} \alpha_{11}-\lambda & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22}-\lambda & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn}-\lambda \end{pmatrix}.$$

Le déterminant de la matrice $A - \lambda E$, noté $|A - \lambda E|$, est un polynôme de degré n par rapport à λ. En effet, le produit des éléments de la diagonale principale est un polynôme par rapport à λ qui est de la forme

$$(-1)^n \lambda^n + \dots;$$

les termes omis sont ceux qui contiennent λ à des puissances strictement inférieures à n; les autres termes du déterminant en question peuvent contenir, au plus, $(n-2)$ éléments de la diagonale principale et, par conséquent, sont des polynômes de degré $n-2$ au plus par rapport à λ. On peut calculer les coefficients du polynôme en question. Ainsi, le coefficient de λ^{n-1} est égal à $(-1)^{n-1}(\alpha_{11} + \alpha_{22} + \dots + \alpha_{nn})$, tandis que le terme indépendant de λ est égal au déterminant de A.

$| A - \lambda E |$, polynôme de degré n par rapport à λ, est appelé *polynôme caractéristique* de la matrice A, et on appelle *racines caractéristiques* de A les zéros (réels ou complexes) du polynôme $| A - \lambda E |$.

Les matrices semblables ont les mêmes polynômes caractéristiques et, par conséquent, les mêmes racines caractéristiques.

En effet, soit

$$B = Q^{-1}AQ.$$

Alors, étant donné que λE commute avec toute matrice Q et que $|Q^{-1}| = |Q|^{-1}$, il vient:

$$|B - \lambda E| = |Q^{-1}AQ - \lambda E| = |Q^{-1}(A - \lambda E)Q| = \\ = |Q|^{-1} \cdot |A - \lambda E| \cdot |Q| = |A - \lambda E|,$$

ce qu'il fallait démontrer.

Ce résultat et le théorème du § 31 sur les matrices d'une application linéaire rapportée à des bases différentes entraînent la proposition suivante: *bien que les matrices d'une application linéaire* φ *rapportée à des bases différentes soient, en général, distinctes, elles ont toutes les mêmes racines caractéristiques.* Il est donc correct de les appeler *racines caractéristiques de l'application linéaire* φ. L'ensemble des racines caractéristiques de φ, où chaque racine est prise autant de fois que l'indique son ordre de multiplicité, est appelé spectral ou *spectre* de l'application linéaire φ.

Les racines caractéristiques jouent un rôle très important dans l'étude des applications linéaires. Le lecteur aura souvent l'occasion de s'en rendre compte. Nous allons donner une des applications des racines caractéristiques.

Soit φ une application linéaire donnée dans un espace vectoriel réel V_n. Soit b un vecteur non nul de V_n tel que son image par l'application φ soit colinéaire à b, c'est-à-dire

$$b\varphi = \lambda_0 b, \tag{1}$$

où λ_0 est réel. Alors, le vecteur b est dit *vecteur propre* et le scalaire réel λ_0 *valeur propre* de l'application linéaire φ; en outre, on dit que le vecteur propre b est *relatif* à la valeur propre λ_0.

Il faut remarquer que le nombre λ_0 est bien défini par la relation (1), car $b \neq 0$. Notons qu'un vecteur propre est toujours non nul, bien que le vecteur nul satisfasse à la condition (1) avec λ_0 quelconque.

La rotation d'un plan euclidien autour de l'origine d'un angle différent de πm avec m entier est un exemple d'application linéaire ne possédant pas de vecteurs propres. L'homothétie d'un plan de coefficient 5 est un exemple de nature entièrement différente. C'est une application linéaire pour laquelle tout vecteur non nul, issu

de l'origine des coordonnées, est propre; tous ces vecteurs sont relatifs à la valeur propre 5.

Une application linéaire φ possède des valeurs propres si et seulement si elle a des racines caractéristiques réelles; en outre, ses valeurs propres coïncident avec les racines caractéristiques réelles correspondantes.

En effet, soient $A = (\alpha_{ij})$ la matrice de l'application φ rapportée à la base $e_1, e_2, \ldots, e_n$ et b,

$$b = \sum_{i=1}^{n} \beta_i e_i,$$

le vecteur propre de φ:

$$b\varphi = \lambda_0 b. \tag{2}$$

On a démontré au § 31 que

$$b\varphi = [(\beta_1, \beta_2, \ldots, \beta_n) A] e. \tag{3}$$

Les relations (2) et (3) nous conduisent au système d'équations

$$\begin{aligned} \beta_1\alpha_{11} + \beta_2\alpha_{21} + \ldots + \beta_n\alpha_{n1} &= \lambda_0\beta_1, \\ \beta_1\alpha_{12} + \beta_2\alpha_{22} + \ldots + \beta_n\alpha_{n2} &= \lambda_0\beta_2, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \beta_1\alpha_{1n} + \beta_2\alpha_{2n} + \ldots + \beta_n\alpha_{nn} &= \lambda_0\beta_n. \end{aligned} \tag{4}$$

Etant donné que $b \neq 0$, les nombres $\beta_1, \beta_2, \ldots, \beta_n$ ne sont pas tous nuls, de sorte que le système d'équations linéaires homogènes (4), qu'on peut mettre sous la forme

$$\begin{aligned} (\alpha_{11} - \lambda_0) x_1 + \alpha_{21}x_2 + \ldots + \alpha_{n1}x_n &= 0, \\ \alpha_{12}x_1 + (\alpha_{22} - \lambda_0) x_2 + \ldots + \alpha_{n2}x_n &= 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha_{1n}x_1 + \alpha_{2n}x_2 + \ldots + (\alpha_{nn} - \lambda_0) x_n &= 0, \end{aligned} \tag{5}$$

possède une solution non nulle. Ceci entraîne que son déterminant doit être nécessairement nul:

$$\begin{vmatrix} \alpha_{11} - \lambda_0, & \alpha_{21}, & \ldots, & \alpha_{n1} \\ \alpha_{12}, & \alpha_{22} - \lambda_0, & \ldots, & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n}, & \alpha_{2n}, & \ldots, & \alpha_{nn} - \lambda_0 \end{vmatrix} = 0. \tag{6}$$

Transposant ce dernier, il vient

$$|A - \lambda_0 E| = 0, \tag{7}$$

ce qui signifie que la valeur propre λ_0 est en même temps une racine caractéristique de la matrice A et, par conséquent, de l'application linéaire φ; en outre, λ_0 est manifestement réel.

Réciproquement, soit λ_0 une racine caractéristique réelle de l'application φ et, par conséquent, de la matrice A. L'égalité (7) a donc lieu, ainsi que l'égalité (6), qui s'obtient de (7) par transposition. Il en résulte que le système (5) possède une solution non nulle; en outre, on peut trouver une solution réelle de ce système, car tous les coefficients de (5) sont réels. Notant par

$$(\beta_1, \beta_2, \ldots, \beta_n) \qquad (8)$$

cette solution, on a les égalités (4). Notons par b le vecteur de V_n qui, rapporté à la base $e_1, e_2, \ldots, e_n$, a pour ligne des coordonnées la ligne (8); il est clair que $b \neq 0$. Alors la relation (3) est vérifiée; les égalités (3) et (4) entraînent la relation (2). L'application φ a donc le vecteur b pour vecteur propre relatif à la valeur propre λ_0. Le théorème est démontré.

Il faut remarquer que dans le cas où l'espace vectoriel V_n est *complexe*, les racines caractéristiques ne sont pas forcément réelles. Autrement dit, dans ce cas, nous aurions démontré le théorème suivant: *soit une application linéaire φ donnée dans un espace vectoriel complexe V_n; alors les racines caractéristiques de φ coïncident avec les valeurs propres correspondantes de l'application φ*. Il en résulte que *toute application linéaire donnée dans un espace vectoriel complexe possède des vecteurs propres.*

Revenons au cas réel étudié ci-dessus. Il faut remarquer que l'ensemble des vecteurs propres relatifs à la valeur propre λ_0 d'une application linéaire φ coïncide avec l'ensemble des solutions réelles non nulles du système d'équations linéaires homogènes (5). Il en résulte qu'*en ajoutant le vecteur nul à l'ensemble des vecteurs propres relatifs à la valeur propre λ_0, nous obtenons un sous-espace vectoriel de l'espace V_n*. En effet, les résultats du § 12 montrent que *l'ensemble de toutes les solutions réelles d'un système d'équations linéaires homogènes à n inconnues est un sous-espace vectoriel de V_n*.

Applications linéaires à spectre simple. Il y a des situations où il est important de savoir s'il existe pour une application linéaire donnée φ une base telle que la matrice de φ, rapportée à cette base, soit *diagonale*. En effet, ce n'est pas toute application linéaire qui, rapportée à une base, puisse avoir pour matrice une matrice diagonale. Les conditions nécessaires et suffisantes seront données au § 61; pour le moment nous ne donnons qu'une condition suffisante. Démontrons d'abord les résultats auxiliaires suivants:

Pour qu'une application linéaire φ, rapportée à une base $e_1, e_2, \ldots, e_n$, ait une matrice diagonale, il faut et il suffit que tout vecteur de cette base soit un vecteur propre de φ.

En effet, les égalités

$$e_i\varphi = \lambda_i e_i$$

sont équivalentes à la condition que la matrice de l'application φ, rapportée à la base $e_1, e_2, \ldots, e_n$, soit diagonale, les éléments diagonaux étant respectivement $\lambda_1, \lambda_2, \ldots, \lambda_n$.

Les vecteurs propres $b_1, b_2, \ldots, b_k$ *d'une application linéaire* φ, *relatifs aux valeurs propres distinctes, forment une famille libre.*

Démontrons cette proposition par récurrence sur k; pour $k=1$ la proposition est vraie, car, tout vecteur propre étant non nul, ce vecteur forme une famille libre. Soient

$$b_i\varphi=\lambda_i b_i, \qquad i=1, 2, \ldots, k,$$

et

$$\lambda_i \neq \lambda_j \quad \text{pour} \quad i \neq j.$$

Si la famille $b_1, b_2, \ldots, b_k$ est non libre,

$$\alpha_1 b_1+\alpha_2 b_2+\ldots+\alpha_k b_k=0, \tag{9}$$

avec, par exemple, $\alpha_1 \neq 0$, alors appliquant φ aux deux membres de l'égalité (9), il vient:

$$\alpha_1\lambda_1 b_1+\alpha_2\lambda_2 b_2+\ldots+\alpha_k\lambda_k b_k=0.$$

Multipliant, l'égalité (9) par λ_k et la retranchant de la dernière égalité, on obtient

$$\alpha_1(\lambda_1-\lambda_k)b_1+\alpha_2(\lambda_2-\lambda_k)b_2+\ldots+\alpha_{k-1}(\lambda_{k-1}-\lambda_k)b_{k-1}=0.$$

Cela signifie que les vecteurs $b_1, b_2, \ldots, b_{k-1}$ forment une famille non libre, car $\alpha_1(\lambda_1-\lambda_k)\neq 0$.

On dit qu'une application linéaire φ donnée dans un espace vectoriel réel V_n a un *spectre simple* si toutes ses racines caractéristiques sont réelles et distinctes. L'application φ a, donc, n valeurs propres distinctes, de sorte que, en vertu du théorème démontré ci-dessus, il existe dans l'espace V_n une base formée par les vecteurs propres de cette application. Ainsi, *toute application linéaire à spectre simple peut être donnée par une matrice diagonale.*

Passant de l'application linéaire aux matrices qui la définissent, nous obtenons le résultat suivant:

Toute matrice dont toutes les racines caractéristiques sont réelles et distinctes est semblable à une matrice diagonale ou, encore, est réductible à la forme diagonale.

Chapitre VIII ESPACES EUCLIDIENS

§ 34. Définition des espaces euclidiens. Bases orthonormales

La notion d'espace vectoriel à n dimensions ne généralise pas, dans une mesure complète, celle de plan ou d'espace euclidien à trois dimensions ; en effet, la longueur d'un vecteur, ni l'angle des deux vecteurs n'étant pas définis pour $n > 3$, il est impossible de développer dans ce cas la théorie géométrique très riche qui est bien connue du lecteur pour $n = 2$ et $n = 3$. Néanmoins cette situation peut être redressée de la manière suivante.

On sait du cours de géométrie analytique que l'on peut introduire dans un plan ou dans un espace à trois dimensions le produit scalaire des vecteurs. Cette définition utilise la notion de longueur des vecteurs et celle d'angle de deux vecteurs ; mais il se révèle, par la suite, que la longueur d'un vecteur aussi bien que l'angle de deux vecteurs peuvent être exprimés au moyen du produit scalaire. Ainsi, utilisant les propriétés bien connues du produit scalaire des vecteurs du plan ou de l'espace à trois dimensions, nous définirons d'abord de facon axiomatique le produit scalaire des vecteurs d'un espace vectoriel à n dimensions. En outre, nous n'introduirons pas la notion de longueur d'un vecteur, ni celle d'angle de deux vecteurs compte tenu de ce qui nous a poussés à inclure ce chapitre dans le cours d'algèbre supérieure. Nous renvoyons le lecteur désireux d'apprendre les fondements de la géométrie dans les espaces à n dimensions à la littérature spéciale et, notamment, aux cours plus complets d'algèbre linéaire.

Notons que partout dans ce chapitre, excepté la fin de ce paragraphe, les espaces vectoriels sont supposés *réels*.

Nous dirons qu'un *produit scalaire* est défini dans un espace vectoriel V_n à n dimensions si à tout couple de vecteurs a et b on associe un nombre réel (noté (a, b) et dit *produit scalaire* des vecteurs a et b) tel que les conditions suivantes soient vérifiées :

I. $$(a, b) = (b, a).$$

II. $$(a + b, c) = (a, c) + (b, c).$$

III. $$(\alpha a, b) = \alpha (a, b).$$

IV. Si $a \neq 0$, alors le produit scalaire de a par a est strictement positif,

$$(a, a) > 0.$$

Ici a, b, c sont des vecteurs de l'espace V_n et α un nombre réel.

Faisant $\alpha = 0$ dans III, il vient :

$$(0, b) = 0, \tag{1}$$

autrement dit, *le produit scalaire du vecteur nul par tout vecteur b est nul*; en particulier, le produit scalaire du vecteur nul par lui-même est nul.

Il résulte immédiatement des II et III la *formule pour le produit scalaire des combinaisons linéaires des vecteurs de deux familles*:

$$\left(\sum_{i=1}^{k} \alpha_i a_i, \sum_{j=1}^{l} \beta_j b_j\right) = \sum_{i=1}^{k} \sum_{j=1}^{l} \alpha_i \beta_j (a_i, b_j). \tag{2}$$

Un espace vectoriel à n dimensions, muni d'un produit scalaire, est dit *espace euclidien* à n dimensions.

Quel que soit n, on peut définir dans un espace vectoriel V_n un produit scalaire, c'est-à-dire transformer V_n en un espace euclidien.

En effet, soit $e_1, e_2, \ldots, e_n$ une base de V_n. Si

$$a = \sum_{i=1}^{n} \alpha_i e_i, \quad b = \sum_{i=1}^{n} \beta_i e_i,$$

on pose

$$(a, b) = \sum_{i=1}^{n} \alpha_i \beta_i. \tag{3}$$

On vérifie aisément que les conditions I-IV sont satisfaites, c'est-à-dire que l'égalité (3) définit dans V_n un produit scalaire.

La définition (3) dépendant manifestement du choix de la base, nous constatons qu'il existe une multitude de façons d'introduire le produit scalaire dans un espace vectoriel à n dimensions ; or, pour le moment, nous ne savons pas encore si nous sommes en mesure d'introduire un produit scalaire de façon essentiellement différente. Nous nous proposons d'examiner toutes les façons de transformer un espace vectoriel à n dimensions en un espace euclidien ; cela nous amènera à la conclusion que, dans un certain sens, il n'existe pour tout n qu'un seul espace euclidien à n dimensions.

Soit E_n un espace euclidien à n dimensions, c'est-à-dire supposons que l'espace vectoriel à n dimensions soit muni d'un produit scalaire quelconque. Les vecteurs a et b sont dits *orthogonaux* si leur produit scalaire est nul :

$$(a, b) = 0.$$

Il résulte de (1) que le vecteur nul est orthogonal à tout vecteur; néanmoins, il existe des vecteurs orthogonaux non nuls.

Une famille de vecteurs est appelée *famille orthogonale* si tous ses vecteurs sont orthogonaux deux à deux.

Toute famille orthogonale de vecteurs non nuls est libre.

En effet, soit une famille de vecteurs $a_1, a_2, \ldots, a_k$ de E_n telle que $a_i \neq 0$, $i = 1, 2, \ldots, k$, et

$$(a_i, a_j) = 0 \quad \text{pour} \quad i \neq j. \tag{4}$$

Soit

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0;$$

formant alors les produits scalaires des deux membres de la dernière égalité par les vecteurs a_i, $1 \leqslant i \leqslant k$, il vient, en vertu de (1), (2) et (4),

$$\begin{aligned} 0 = (0, a_i) &= (\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k, a_i) = \\ &= \alpha_1 (a_1, a_i) + \alpha_2 (a_2, a_i) + \ldots + \alpha_k (a_k, a_i) = \\ &= \alpha_i (a_i, a_i). \end{aligned}$$

Il en résulte que $\alpha_i = 0$, $i = 1, 2, \ldots, k$, car, selon IV, $(a_i, a_i) > 0$, ce qu'il fallait démontrer.

A présent, décrivons le *procédé d'orthogonalisation*, c'est-à-dire un moyen de passer d'une famille libre de k vecteurs non nuls

$$a_1, a_2, \ldots, a_k \tag{5}$$

d'un espace euclidien E_n à une famille orthogonale composée également de k vecteurs non nuls de E_n qui seront notés $b_1, b_2, \ldots, b_k$.

Soit $b_1 = a_1$, c'est-à-dire *le premier vecteur de la famille* (5) *sera également un élément de la famille orthogonale que nous devons former.* Posons, ensuite,

$$b_2 = \alpha_1 b_1 + a_2.$$

Le vecteur b_2 n'est pas nul pour toute valeur du nombre réel α_1, car $b_1 = a_1$ et les vecteurs a_1 et a_2 sont linéairement indépendants. Choisissons α_1 de manière que b_2 soit orthogonal à b_1:

$$0 = (b_1, b_2) = (b_1, \alpha_1 b_1 + a_2) = \alpha_1 (b_1, b_1) + (b_1, a_2),$$

d'où, vu la condition IV, on obtient:

$$\alpha_1 = -\frac{(b_1, a_2)}{(b_1, b_1)}.$$

Supposons que nous ayons déjà trouvé une famille orthogonale de l vecteurs non nuls, soit $b_1, b_2, \ldots, b_l$; supposons, en outre, que le vecteur b_i s'exprime linéairement par les vecteurs $a_1, a_2, \ldots, a_i$, $1 \leqslant i \leqslant l$. Cette dernière supposition sera également vraie

pour le vecteur b_{l+1}, s'il est de la forme

$$b_{l+1} = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_l b_l + a_{l+1}.$$

En outre, la famille (5) étant libre et le vecteur a_{l+1} n'intervenant pas dans l'expression des vecteurs $b_1, b_2, \ldots, b_l$, le vecteur b_{l+1} est non nul. Choisissons les coefficients α_i, $i = 1, 2, \ldots, l$, de manière que le vecteur b_{l+1} soit orthogonal aux vecteurs b_i, $i = 1, 2, \ldots, l$,

$$0 = (b_i, b_{l+1}) = (b_i, \alpha_1 b_1 + \alpha_2 b_2 + \ldots \\ \ldots + \alpha_l b_l + a_{l+1}) = \alpha_1 (b_i, b_1) + \\ + \alpha_2 (b_i, b_2) + \ldots + \alpha_l (b_i, b_l) + \\ + (b_i, a_{l+1});$$

les vecteurs $b_1, b_2, \ldots, b_l$ étant orthogonaux, il en résulte que

$$\alpha_i (b_i, b_i) + (b_i, a_{l+1}) = 0$$

ou encore

$$\alpha_i = -\frac{(b_i, a_{l+1})}{(b_i, b_i)}, \qquad i = 1, 2, \ldots, l.$$

Continuant ce processus, nous construirons la famille orthogonale cherchée de vecteurs $b_1, b_2, \ldots, b_k$.

Appliquant le procédé d'orthogonalisation à une base de l'espace E_n, nous obtiendrons une famille orthogonale de n vecteurs non nuls, c'est-à-dire une base *orthogonale* de E_n, les vecteurs en étant linéairement indépendants, en vertu de la proposition démontrée ci-dessus. En outre, étant donné que tout vecteur non nul appartient à une base et compte tenu de la remarque ci-dessus sur le premier pas du procédé d'orthogonalisation, nous pouvons énoncer la proposition suivante:

Tout espace euclidien possède des bases orthogonales; en outre, tout vecteur non nul de cet espace appartient à une base orthogonale.

Dans la suite, un rôle important est attribué à un type spécial de bases orthogonales; ces bases correspondent aux coordonnées cartésiennes, utilisées en géométrie analytique.

Un vecteur b est dit *normé* si le produit scalaire de b par lui-même est égal à l'unité:

$$(b, b) = 1.$$

Le passage d'un vecteur $a \neq 0$ (et, par suite, $(a, a) > 0$) au vecteur

$$b = \frac{1}{\sqrt{(a, a)}} a$$

s'appelle *normalisation* du vecteur a. Le vecteur b est déjà normé, car

$$(b, b) = \left(\frac{1}{\sqrt{(a, a)}} a, \frac{1}{\sqrt{(a, a)}} a\right) = \left(\frac{1}{\sqrt{(a, a)}}\right)^2 (a, a) = 1.$$

Une base $e_1, e_2, \ldots, e_n$ d'un espace euclidien E_n est dite *orthonormale* si elle est orthogonale et si tout vecteur e_j de cette base est normé :

$$\begin{aligned} &(e_i, e_j) = 0 \text{ pour } i \neq j, \\ &(e_i, e_i) = 1, \qquad i = 1, 2, \ldots, n. \end{aligned} \tag{6}$$

Tout espace euclidien possède des bases orthonormales.

Pour démontrer cela, il suffit de normer les vecteurs d'une base orthogonale. La base restera orthogonale, car si $(a, b) = 0$, alors

$$(\alpha a, \beta b) = \alpha\beta (a, b) = 0,$$

pour tous nombres α et β.

Pour qu'une base $e_1, e_2, \ldots, e_n$ d'un espace euclidien E_n soit orthonormale, il faut et il suffit que pour tout couple de vecteurs de E_n rapportés à cette base leur produit scalaire soit égal à la somme des produits des coordonnées de même indice de ces vecteurs; *autrement dit, les égalités*

$$a = \sum_{i=1}^{n} \alpha_i e_i, \qquad b = \sum_{j=1}^{n} \beta_j e_j \tag{7}$$

entraînent

$$(a, b) = \sum_{i=1}^{n} \alpha_i \beta_i \tag{8}$$

et inversement.

En effet, si la base en question vérifie les égalités (6), alors

$$(a, b) = \left(\sum_{i=1}^{n} \alpha_i e_i, \sum_{j=1}^{n} \beta_j e_j\right) = \sum_{i, j=1}^{n} \alpha_i \beta_j (e_i, e_j) = \sum_{i=1}^{n} \alpha_i \beta_i.$$

Réciproquement, si la base $e_1, e_2, \ldots, e_n$ est telle que pour tout couple de vecteurs a et b ayant la forme (7) le produit scalaire (a, b) s'exprime par la formule (8), alors, prenant pour a et b les vecteurs e_i et e_j avec $1 \leqslant i, j \leqslant n$, nous déduirons de (8) les égalités (6).

Comparant ce résultat à la démonstration du théorème d'existence des espaces euclidiens à n dimensions pour tout n (cf. ci-dessus),

nous pouvons énoncer la proposition suivante: *soit une base dans un espace vectoriel V_n à n dimensions; alors on peut munir V_n d'un produit scalaire tel que la base choisie soit une base orthonormale de l'espace euclidien correspondant.*

Isomorphisme d'espaces euclidiens. Les espaces euclidiens E et E' sont dits *isomorphes* s'il existe une application bijective de E sur E' telle que les conditions suivantes soient vérifiées:

1) cette application est un isomorphisme de E sur E', en tant qu'espaces vectoriels (cf. § 29);

2) cette application conserve le produit scalaire, autrement dit, si les vecteurs a' et b' de E' sont respectivement images des vecteurs a et b de E, alors

$$(a, b) = (a', b'). \tag{9}$$

Il résulte immédiatement de la condition 1) que *deux espaces euclidiens isomorphes ont la même dimension.* Montrons la réciproque.

Si E et E' sont deux espaces euclidiens à n dimensions, alors ils sont isomorphes.

En effet, soient

$$e_1, e_2, \ldots, e_n \tag{10}$$

et

$$e'_1, e'_2, \ldots, e'_n \tag{11}$$

les bases *orthonormales* respectivement de E et E'. Faisant correspondre à tout vecteur a de E:

$$a = \sum_{i=1}^{n} \alpha_i e_i$$

le vecteur a' de E'

$$a' = \sum_{i=1}^{n} \alpha_i e'_i$$

(a et a' rapportés respectivement aux bases (10) et (11) ont les mêmes coordonnées), nous obtenons manifestement un isomorphisme des espaces vectoriels E et E'. Montrons que l'égalité (9) a lieu; en effet, si

$$b = \sum_{i=1}^{n} \beta_i e_i, \qquad b' = \sum_{i=1}^{n} \beta_i e'_i,$$

alors, selon (8), il vient (les bases (10) et (11) sont orthonormales!):

$$(a, b) = \sum_{i=1}^{n} \alpha_i \beta_i = (a', b').$$

Il est naturel de ne pas distinguer les espaces euclidiens isomorphes. Ainsi, pour tout n, il n'y a qu'un seul espace euclidien à n dimensions, de même que pour tout n il n'existe qu'un seul espace vectoriel à n dimensions.

Les notions et les résultats de ce paragraphe peuvent être généralisés au cas des espaces vectoriels *complexes*. Un espace vectoriel complexe est appelé *espace euclidien complexe* s'il est muni d'un produit scalaire (a, b), le nombre (a, b) étant, en général, complexe; le produit scalaire doit vérifier les axiomes II-IV (dans l'énoncé du dernier axiome il faut souligner que le produit scalaire d'un vecteur b non nul par lui-même est réel et strictement positif), tandis que l'axiome I doit être remplacé par la condition :

I′ $$(a, b) = \overline{(b, a)},$$

où la barre signifie, comme d'habitude, le passage au nombre conjugué complexe.

Par conséquent, le produit scalaire n'est plus commutatif. Néanmoins, l'égalité symétrique de celle de l'axiome II est encore valable

II′ $$(a, b+c) = (a, b) + (a, c),$$

car

$$(a, b+c) = \overline{(b+c, a)} = \overline{(b, a)+(c, a)} = \overline{(b, a)} + \overline{(c, a)} = (a, b) + (a, c).$$

D'autre part,

III′ $$(a, \alpha b) = \bar{\alpha}(a, b),$$

car

$$(a, \alpha b) = \overline{(\alpha b, a)} = \overline{\alpha (b, a)} = \bar{\alpha}\,\overline{(b, a)} = \bar{\alpha}(a, b).$$

Les notions d'orthogonalité et de famille orthonormale de vecteurs se généralisent sans aucun changement au cas des espaces euclidiens complexes. On démontre, tout comme dans le cas réel, l'existence de bases orthonormales dans un espace euclidien complexe à un nombre fini de dimensions. Toutefois, si $e_1, e_2, \ldots, e_n$ est une base orthonormale et si les vecteurs a et b, rapportés à cette base, ont la forme (7), alors

$$(a, b) = \sum_{i=1}^{n} \alpha_i \overline{\beta_i}.$$

Les résultats des paragraphes suivants s'étendent également au cas des espaces euclidiens complexes. Toutefois, nous ne nous en occuperons pas ici et nous renvoyons le lecteur qui s'y intéresse aux livres spéciaux d'algèbre linéaire.

§ 35. Matrices orthogonales, applications orthogonales

Soit une transformation linéaire réelle de n indéterminées à coefficients réels :

$$x_i = \sum_{k=1}^{n} q_{ik} y_k, \qquad i = 1, 2, \ldots, n. \tag{1}$$

Notons par Q sa matrice. Cette transformation associe à la somme des carrés des indéterminées $x_1, x_2, \ldots, x_n$, c'est-à-dire à la forme

quadratique $x_1^2 + x_2^2 + \ldots + x_n^2$, une forme quadratique des indéterminées $y_1, y_2, \ldots, y_n$. Il peut arriver que cette dernière soit également une somme des carrés des indéterminées $y_1, y_2, \ldots, y_n$, c'est-à-dire que l'on ait, après avoir remplacé $x_1, x_2, \ldots, x_n$ par leurs expressions (1), l'identité

$$x_1^2 + x_2^2 + \ldots + x_n^2 = y_1^2 + y_2^2 + \ldots + y_n^2. \tag{2}$$

Une transformation linéaire des indéterminées (1) jouissant de cette propriété, c'est-à-dire conservant la somme des carrés des indéterminées, s'appelle *transformation orthogonale* et sa matrice Q est dite *matrice orthogonale.*

Il y a d'autres définitions équivalentes des transformations et matrices orthogonales. Donnons-en quelques-unes qui sont nécessaires pour la suite.

On connaît du § 26 la règle selon laquelle se transforme la matrice d'une forme quadratique lorsqu'on fait une transformation linéaire des indéterminées. En l'appliquant dans notre cas, nous obtenons, vu que la matrice unité E est la matrice de la forme quadratique, somme des carrés des indéterminées, une égalité matricielle équivalente à (2)

$$Q'EQ = E$$

ou encore

$$Q'Q = E, \tag{3}$$

d'où l'on a

$$Q' = Q^{-1}, \tag{4}$$

de sorte que l'on a aussi

$$QQ' = E. \tag{5}$$

Ainsi, en vertu de (4), on peut dire que *la matrice Q est orthogonale si sa transposée Q' est égale à son inverse Q^{-1}*. Chacune des égalités (3) et (5) peut être admise comme définition des matrices orthogonales.

Les colonnes de la matrice Q' étant les lignes correspondantes de la matrice Q, on déduit de (5) la proposition suivante : *une matrice carrée Q est orthogonale si et seulement si la somme des carrés des éléments d'une ligne quelconque de Q est égale à l'unité et si la somme des produits des éléments d'une ligne quelconque par les éléments correspondants d'une autre ligne quelconque est nulle.* Il résulte de (3) la même proposition pour les colonnes de la matrice Q.

Passant dans (3) aux déterminants, il vient :

$$|Q|^2 = 1,$$

car $|Q'| = |Q|$. On en déduit que *le déterminant d'une matrice orthogonale est* ± 1. Ainsi, *toute transformation orthogonale des indéterminées est non dégénérée* [1]. Bien entendu, la réciproque n'est pas vraie; en outre, ce n'est pas toute matrice à déterminant ± 1 qui sera orthogonale.

L'inverse d'une matrice orthogonale est également une matrice orthogonale. En effet, passant dans (4) aux matrices transposées, il vient:

$$(Q^{-1})' = (Q')' = Q = (Q^{-1})^{-1}.$$

D'autre part, *le produit de matrices orthogonales est une matrice orthogonale.* En effet, soient Q et R deux matrices orthogonales; utilisant (4), ainsi que l'égalité (6) du § 26 et l'égalité analogue pour la matrice inverse, nous obtenons:

$$(QR)' = R'Q' = R^{-1}Q^{-1} = (QR)^{-1}.$$

La proposition suivante sera utilisée au § 37:

La matrice de passage d'une base orthonormale dans un espace euclidien à une autre base orthonormale dans ce même espace est orthogonale.

En effet, soient $e_1, e_2, \ldots, e_n$ et $e'_1, e'_2, \ldots, e'_n$ deux bases orthonormales sur E_n et $Q = (q_{ij})$ la matrice de passage de e à e':

$$e' = Qe.$$

La base e étant orthonormale, le produit scalaire de tout couple de vecteurs de E_n et, en particulier, de deux vecteurs de la base e', est égal à la somme des produits des coordonnées de même indice de ces vecteurs rapportés à la base e. Or, la base e' étant aussi orthonormale, le produit scalaire de tout vecteur de e' par lui-même est égal à l'unité, tandis que le produit scalaire de tout couple de vecteurs distincts de e' est nul. Il en résulte que les lignes des coordonnées des vecteurs de la base e', rapportés à la base e, c'est-à-dire les lignes de la matrice Q, vérifient les égalités qui ont été déduites de l'égalité (5) et caractérisent les matrices orthogonales.

Applications orthogonales dans un espace euclidien. Maintenant, il est commode de passer à l'étude d'un type spécial d'applications linéaires des espaces euclidiens, bien que ce type d'applications ne soit pas ensuite utilisé.

Une application linéaire φ d'un espace euclidien E_n est appelée *application orthogonale sur E_n*, si elle conserve le produit scalaire de tout vecteur a par lui-même, c'est-à-dire si

$$(a\varphi, a\varphi) = (a, a). \qquad (6)$$

---

[1] En fait, cela résulte déjà de l'égalité (3). (*N.d.T.*)

On en déduit une proposition plus générale, qui, comme il va de soi, peut être également admise comme définition d'une application orthogonale. Voici cette proposition:

Une application orthogonale φ *sur un espace euclidien conserve le produit scalaire de tout couple de vecteurs* a *et* b *de cet espace*

$$(a\varphi,\ b\varphi) = (a,\ b). \tag{7}$$

En effet, en vertu de (6), on a

$$((a+b)\varphi,\ (a+b)\varphi) = (a+b,\ a+b).$$

D'un autre côté,

$$((a+b)\varphi,\ (a+b)\varphi) = (a\varphi + b\varphi, a\varphi + b\varphi) =$$
$$= (a\varphi,\ a\varphi) + (a\varphi,\ b\varphi) + (b\varphi,\ a\varphi) + (b\varphi,\ b\varphi),$$
$$(a+b,\ a+b) = (a,\ a) + (a,\ b) + (b,\ a) + (b,\ b).$$

Utilisant (6) aussi bien pour a que pour b et compte tenu de la commutativité du produit scalaire, on en déduit l'égalité

$$2\,(a\varphi,\ b\varphi) = 2\,(a,\ b),$$

d'où la relation (7).

L'image de toute base orthonormale sur un espace euclidien par une application orthogonale est encore une base orthonormale de cet espace. Inversement, supposons qu'une application linéaire sur un espace euclidien transforme au moins une seule base orthonormale en une base orthonormale; alors, cette application est une application orthogonale.

En effet, soient φ une application orthogonale et $e_1,\ e_2,\ \ldots,\ e_n$ une base orthonormale sur E_n. Compte tenu de (7), on déduit des égalités

$$(e_i,\ e_i) = 1, \qquad i = 1,\ 2,\ \ldots,\ n,$$
$$(e_i,\ e_j) = 0 \quad \text{pour} \quad i \neq j$$

les égalités

$$(e_i\varphi,\ e_i\varphi) = 1, \qquad i = 1,\ 2,\ \ldots,\ n,$$
$$(e_i\varphi,\ e_j\varphi) = 0 \quad \text{pour} \quad i \neq j;$$

autrement dit, la famille de vecteurs $e_1\varphi,\ e_2\varphi,\ \ldots,\ e_n\varphi$ est orthonormale, de sorte que ces vecteurs forment une base orthonormale de E_n.

Réciproquement, soient φ une application linéaire et $e_1,\ e_2,\ \ldots$ $\ldots,\ e_n$ une base orthonormale de E_n telle que l'image de cette base, soit $e_1\varphi,\ e_2\varphi,\ \ldots,\ e_n\varphi$, par l'application φ, soit encore une base

orthonormale de E_n. Si

$$a=\sum_{i=1}^{n}\alpha_i e_i$$

est un vecteur quelconque de l'espace E_n, alors

$$a\varphi=\sum_{i=1}^{n}\alpha_i(e_i\varphi),$$

c'est-à-dire le vecteur $a\varphi$, rapporté à la base $e\varphi$, a les mêmes coordonnées que le vecteur a rapporté à la base e. Or, les deux bases sont orthonormales, de sorte que le produit scalaire de tout vecteur par lui-même est égal à la somme des carrés de ses coordonnées, et cela indépendamment de la base orthonormale choisie dans E_n. Ainsi

$$(a,\ a)=(a\varphi,\ a\varphi)=\sum_{i=1}^{n}\alpha_i^2,$$

c'est-à-dire l'égalité (6) a lieu.

Une application orthogonale sur un espace euclidien, rapportée à toute base orthonormale, a pour matrice une matrice orthogonale. Inversement, supposons qu'une application linéaire sur un espace euclidien, rapportée à une base orthonormale donnée, a pour matrice une matrice orthogonale; alors, cette application est orthogonale.

En effet, soient φ une application orthogonale et $e_1, e_2, \ldots, e_n$ une base orthonormale; alors, la famille de vecteurs $e_1\varphi, e_2\varphi, \ldots, e_n\varphi$ est aussi une base orthonormale. La matrice A de l'application φ, rapportée à la base e,

$$e\varphi=Ae \tag{8}$$

est, donc, la matrice de passage de la base orthonormale e à la base orthonormale $e\varphi$; par conséquent, d'après la proposition démontrée ci-dessus, A est une matrice orthogonale.

Inversement, soient une application linéaire φ et une base orthonormale $e_1, e_2, \ldots, e_n$; supposons que la matrice A de l'application φ rapportée à la base e soit orthogonale. Alors l'égalité (8) a lieu. La base e étant orthonormale, le produit scalaire de tout couple de vecteurs de E_n et, en particulier, de deux vecteurs de la famille $e_1\varphi, e_2\varphi, \ldots, e_n\varphi$, est égal à la somme des produits des coordonnées de même indice de ces vecteurs (les vecteurs sont rapportés à la base e). Ainsi, la matrice A étant orthogonale, on a

$$(e_i\varphi,\ e_i\varphi)=1,\qquad i=1,\ 2,\ \ldots,\ n,$$
$$(e_i\varphi,\ e_j\varphi)=0\quad \text{pour}\quad i\neq j,$$

c'est-à-dire la famille $e\varphi$ est une base orthonormale de l'espace E_n. Il en résulte que φ est une application orthogonale.

Le lecteur sait du cours de géométrie analytique que parmi toutes les applications linéaires du plan dans lui-même les rotations sont les seules à conserver le produit scalaire des vecteurs (il faut y ajouter aussi les symétries par rapport aux droites). Ainsi, par analogie, les applications orthogonales dans un espace euclidien à n dimensions peuvent être considérées comme les « rotations » de cet espace.

Il est clair que l'application identique dans un espace euclidien est une application orthogonale. D'autre part, la relation établie ci-dessus, entre les applications orthogonales et les matrices orthogonales, ainsi que les résultats du § 31, concernant les opérations sur les applications linéaires et les matrices, permettent d'établir, en partant des propriétés déjà connues des matrices orthogonales, les propriétés correspondantes des applications orthogonales.

Toute application orthogonale est une application linéaire non dégénérée et son inverse est aussi une application orthogonale.

Le produit d'applications orthogonales est encore une application orthogonale.

D'ailleurs, ces propositions peuvent être vérifiées directement.

§ 36. Applications symétriques

Une application linéaire φ d'un espace euclidien à n dimensions est dite application *symétrique* (ou *auto-adjointe*) si pour tout couple de vecteurs a et b de l'espace on a

$$(a\varphi, b) = (a, b\varphi), \tag{1}$$

autrement dit, dans un produit scalaire on peut faire passer une application symétrique du premier facteur au second.

Il est clair que l'application identique ε et l'application nulle ω sont des exemples d'applications symétriques. Un autre exemple, moins banal, est donné par l'application linéaire qui à tout vecteur a de l'espace fait correspondre le vecteur αa, α étant un nombre réel fixe,

$$a\varphi = \alpha a.$$

En effet, on a dans ce cas

$$(a\varphi, b) = (\alpha a, b) = \alpha (a, b) = (a, \alpha b) = (a, b\varphi).$$

Le rôle joué par les applications symétriques est très important, et nous devons les étudier en détail.

Une application symétrique dans un espace euclidien, rapportée à une base orthonormale quelconque, a pour matrice une matrice symétrique. Inversement, si une application linéaire dans un espace euclidien, rapportée au moins à une seule base orthonormale, donne une matrice symétrique, alors cette application est symétrique.

En effet, soit $A = (\alpha_{ij})$ la matrice d'une application symétrique φ rapportée à une base $e_1, e_2, \ldots, e_n$. Etant donné que le produit scalaire de deux vecteurs, rapportés à une base orthonormale, est égal à la somme des produits des coordonnées de même indice, il vient :

$$(e_i\varphi, e_j) = \Big(\sum_{k=1}^{n} \alpha_{ik}e_k, e_j\Big) = \alpha_{ij},$$

$$(e_i, e_j\varphi) = \Big(e_i, \sum_{k=1}^{n} \alpha_{jk}e_k\Big) = \alpha_{ji},$$

c'est-à-dire, en vertu de (1), on a pour i et j quelconques

$$\alpha_{ij} = \alpha_{ji}.$$

Ainsi la matrice A est symétrique.

Inversement, supposons que la matrice $A = (\alpha_{ij})$ d'une application φ, rapportée à une base orthonormale $e_1, e_2, \ldots, e_n$, soit symétrique, c'est-à-dire que

$$\alpha_{ij} = \alpha_{ji} \quad \text{pour tous} \quad i, j. \tag{2}$$

Soient b et c deux vecteurs de l'espace euclidien, qui, rapportés à la base e, sont de la forme

$$b = \sum_{i=1}^{n} \beta_i e_i, \quad c = \sum_{j=1}^{n} \gamma_j e_j.$$

Alors

$$b\varphi = \sum_{i=1}^{n} \beta_i (e_i\varphi) = \sum_{j=1}^{n} \Big(\sum_{i=1}^{n} \beta_i \alpha_{ij}\Big) e_j,$$

$$c\varphi = \sum_{j=1}^{n} \gamma_j (e_j\varphi) = \sum_{i=1}^{n} \Big(\sum_{j=1}^{n} \gamma_j \alpha_{ji}\Big) e_i.$$

Compte tenu de ce que la base e est orthonormale, il vient :

$$(b\varphi, c) = \sum_{j,\, i=1}^{n} \beta_i \alpha_{ij} \gamma_j,$$

$$(b, c\varphi) = \sum_{i,\, j=1}^{n} \beta_i \gamma_j \alpha_{ji}.$$

D'après (2), les seconds membres des deux dernières égalités coïncident, de sorte que l'on a

$$(b\varphi, c) = (b, c\varphi),$$

ce qu'il fallait démontrer.

On déduit du résultat obtenu la propriété suivante des applications symétriques (qui, d'ailleurs, peut être vérifiée directement):

La somme des applications symétriques aussi bien que le produit d'un scalaire par une application symétrique sont encore des applications symétriques.

Démontrons maintenant le théorème important suivant:

Toutes les racines caractéristiques d'une application symétrique sont réelles.

Etant donné que les racines caractéristiques d'une application linéaire φ ont les mêmes valeurs que les racines caractéristiques de la matrice qui s'obtient en rapportant φ à une base quelconque et vu que les applications symétriques rapportées à des bases orthonormales sont données par les matrices symétriques, il suffit de démontrer la proposition suivante:

Toutes les racines caractéristiques d'une matrice symétrique sont réelles.

En effet, soit λ_0 une racine caractéristique, réelle ou complexe, d'une matrice symétrique $A = (\alpha_{ij})$,

$$|A - \lambda_0 E| = 0.$$

Alors, le système d'équations linéaires homogènes à coefficients complexes

$$\sum_{j=1}^{n} \alpha_{ij} x_j = \lambda_0 x_i, \qquad i = 1, 2, \ldots, n,$$

a son déterminant nul, ce qui veut dire que ce système possède une solution *non nulle*, soit $\beta_1, \beta_2, \ldots, \beta_n$, qui est, en général, complexe ; ainsi

$$\sum_{j=1}^{n} \alpha_{ij} \beta_j = \lambda_0 \beta_i, \qquad i = 1, 2, \ldots, n. \tag{3}$$

Multipliant les deux membres de la $i^{\text{ème}}$ égalité (3) par le nombre $\bar{\beta}_i$ conjugué complexe de β_i et les additionnant par rapport à i, il vient:

$$\sum_{i, j=1}^{n} \alpha_{ij} \beta_j \bar{\beta}_i = \lambda_0 \sum_{i=1}^{n} \beta_i \bar{\beta}_i. \tag{4}$$

Le coefficient de λ_0 dans (4) est réel et non nul, car il est égal á la somme de nombres réels non négatifs dont au moins un est non nul. Ainsi, on démontrera que λ_0 est réel si l'on montre que le premier membre dans (4) est un nombre réel. Pour cela il suffit de montrer que ce nombre coïncide avec son conjugué complexe. Ici nous utiliserons pour la première fois le fait que la matrice A

est symétrique (et réelle). On a

$$\overline{\sum_{i,\,j=1}^{n} \alpha_{ij}\beta_j\overline{\beta}_i} = \sum_{i,\,j=1}^{n} \overline{\alpha_{ij}\beta_j\overline{\beta}_i} = \sum_{i,\,j=1}^{n} \alpha_{ij}\overline{\beta}_j\beta_i = \sum_{i,\,j=1}^{n} \alpha_{ji}\overline{\beta}_j\beta_i =$$

$$= \sum_{i,\,j=1}^{n} \alpha_{ij}\overline{\beta}_i\beta_j = \sum_{i,\,j=1}^{n} \alpha_{ij}\beta_j\overline{\beta}_i.$$

Notons que l'avant-dernière égalité a été obtenue en échangeant les indices de sommation i et j. Le théorème est donc démontré.

Une application linéaire φ d'un espace euclidien E_n est une application symétrique si et seulement si il existe dans E_n une base orthonormale formée par les vecteurs propres de φ.

Une partie de cette proposition est presque évidente : s'il existe une base orthonormale $e_1, e_2, \ldots, e_n$ dans E_n telle que

$$e_i\varphi = \lambda_i e_i, \qquad i = 1, 2, \ldots, n,$$

alors la matrice de l'application φ, rapportée à la base e, est diagonale :

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}$$

Or, la matrice diagonale est manifestement symétrique, de sorte que l'application φ, rapportée à la base orthonormale e, a pour matrice une matrice symétrique ; par conséquent, φ est une application symétrique.

Nous allons démontrer la réciproque par récurrence sur la dimension n de l'espace E_n. En effet, pour $n = 1$ l'image de tout vecteur a de l'espace E_1 par une application linéaire φ est colinéaire à a. Il s'ensuit que tout vecteur non nul a de E_1 est un vecteur propre de φ (il en résulte, d'ailleurs, que toute application linéaire est dans ce cas symétrique). Prenant pour a un vecteur normé, nous obtenons la base orthonormale cherchée.

Supposons que le théorème soit démontré pour tout espace euclidien à $(n - 1)$ dimensions, et soit φ une application symétrique dans E_n. Du théorème démontré ci-dessus il résulte l'existence d'une racine caractéristique réelle, soit λ_0, de l'application φ. λ_0 est, donc, une valeur propre de φ. Soit a le vecteur propre de φ relatif à la valeur propre λ_0 ; alors, tout vecteur non nul colinéaire à a est, également, un vecteur propre de φ relatif à la même valeur propre λ_0, car

$$(\alpha a)\varphi = \alpha(a\varphi) = \alpha(\lambda_0 a) = \lambda_0(\alpha a).$$

Prenant, en particulier, un vecteur normé e_1 colinéaire à a, il vient :

$$e_1\varphi = \lambda_0 e_1,$$
$$(e_1, e_1) = 1.$$

Nous avons démontré au § 34 que tout vecteur non nul e_1 de E_n peut être complété en une base orthogonale de E_n :

$$e_1, e'_2, \ldots, e'_n. \tag{5}$$

Les vecteurs de E_n, qui ont dans la base (5) la première coordonnée nulle, c'est-à-dire qui sont de la forme $\alpha_2 e'_2 + \ldots + \alpha_n e'_n$, forment, manifestement, un sous-espace vectoriel à $(n-1)$ dimensions de l'espace E_n qui sera noté L. En outre, L est un espace euclidien à $(n-1)$ dimensions, car le produit scalaire étant défini pour les vecteurs de E_n, il est, en particulier, défini pour les vecteurs de L et jouit de toutes les propriétés requises.

Le sous-espace L est formé par les vecteurs de E_n qui sont orthogonaux au vecteur e_1. En effet, si

$$a = \alpha_1 e_1 + \alpha'_2 e'_2 + \ldots + \alpha'_n e'_n,$$

alors, la base (5) étant orthogonale et le vecteur e_1 normé, on a

$$(e_1, a) = \alpha_1 (e_1, e_1) + \alpha'_2 (e_1, e'_2) + \ldots + \alpha'_n (e_1, e'_n) = \alpha_1,$$

c'est-à-dire $(e_1, a) = 0$ si et seulement si $\alpha_1 = 0$.

Soit a un vecteur du sous-espace L, c'est-à-dire $(e_1, a) = 0$. Alors, le vecteur $a\varphi$ appartient également à L. En effet, l'application φ étant symétrique, on a

$$(e_1, a\varphi) = (e_1\varphi, a) = (\lambda_0 e_1, a) = \lambda_0 (e_1, a) = \lambda_0 \cdot 0 = 0,$$

c'est-à-dire le vecteur $a\varphi$ est orthogonal à e_1 et, par conséquent, appartient à L. On exprime cette propriété du sous-espace L en disant que L est *invariant* par rapport à l'application φ ; elle permet de considérer φ en même temps comme une application linéaire de l'espace euclidien L à $(n-1)$ dimensions sur lui-même. Cette application définit, en outre, une application symétrique dans L, car l'égalité (1), valable pour les vecteurs de E_n, est, en particulier, vraie pour les vecteurs de L.

En vertu de la récurrence, il existe une base orthonormale dans L formée par les vecteurs propres de l'application φ; notons cette base par $e_2, e_3, \ldots, e_n$. Tous ces vecteurs sont orthogonaux au vecteur e_1, de sorte que la famille $e_1, e_2, \ldots, e_n$ est la base orthonormale de E_n, formée par les vecteurs propres de l'application φ. Le théorème est démontré.

§ 37. Réduction d'une forme quadratique à ses axes principaux. Couples de formes quadratiques

Appliquons le dernier théorème du paragraphe précédent pour donner la démonstration du théorème suivant sur les matrices:

Pour toute matrice symétrique A on peut trouver une matrice orthogonale réduisant A à la forme diagonale, c'est-à-dire une matrice orthogonale Q telle que la matrice $Q^{-1}AQ$ soit diagonale.

En effet, soit une matrice symétrique A d'ordre n. Si $e_1, e_2, \ldots, e_n$ est une base orthonormale d'un espace euclidien E_n à n dimensions, alors il existe une application symétrique φ dans E_n telle que φ, rapportée à la base e, soit donnée par la matrice A. On a démontré l'existence d'une base orthonormale dans E_n formée par les vecteurs propres de φ, soit $f_1, f_2, \ldots, f_n$; l'application φ, rapportée à cette base, a pour matrice une matrice diagonale (cf. § 33). Alors, en vertu du § 31, on a

$$B = Q^{-1}AQ, \tag{1}$$

Q étant la matrice de passage de la base f à la base e,

$$e = Qf. \tag{2}$$

En tant que matrice de passage d'une base orthonormale à une autre, Q est orthogonale (cf. § 35). Le théorème est démontré.

La matrice Q étant orthogonale et, par conséquent, son inverse étant égale à sa matrice transposée: $Q^{-1} = Q'$, on peut mettre l'égalité (1) sous la forme suivante:

$$B = Q'AQ.$$

Or, on sait du § 26 que c'est là exactement la loi selon laquelle se transforme la matrice symétrique A d'une forme quadratique soumise à une transformation linéaire des indéterminées de matrice Q. Compte tenu de ce qu'une transformation linéaire des indéterminées de matrice orthogonale est une application orthogonale (cf. § 35) et vu que la matrice diagonale correspond à la forme quadratique réduite à la somme des carrés des indéterminées, nous obtenons, utilisant le dernier théorème, le *théorème* suivant *sur la réduction des formes quadratiques à leurs axes principaux*:

Toute forme quadratique réelle $f(x_1, x_2, \ldots, x_n)$ peut être réduite par une application orthogonale des indéterminées à la forme canonique.

Bien qu'il y ait, en général, plusieurs applications orthogonales réduisant une forme quadratique $f(x_1, x_2, \ldots, x_n)$ à la forme canonique, les coefficients de la forme canonique sont bien définis:

Quelle que soit l'application orthogonale réduisant une forme quadratique $f(x_1, x_2, \ldots, x_n)$ de matrice A à la forme canonique, les coefficients de cette forme canonique sont les racines caractéristiques de la matrice A prises avec leurs ordres de multiplicité.

En effet, supposons que f soit réduite par une application orthogonale à la forme canonique

$$f(x_1, x_2, \ldots, x_n) = \mu_1 y_1^2 + \mu_2 y_2^2 + \ldots + \mu_n y_n^2.$$

La somme des carrés des indéterminées étant invariante par rapport à une application orthogonale, on a

$$f(x_1, x_2, \ldots, x_n) - \lambda \sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n} \mu_i y_i^2 - \lambda \sum_{i=1}^{n} y_i^2,$$

où λ est un paramètre réel. Passant aux déterminants de ces formes quadratiques, il vient :

$$|A - \lambda E| = \begin{vmatrix} \mu_1 - \lambda & 0 & \ldots & 0 \\ 0 & \mu_2 - \lambda & \ldots & 0 \\ \cdot & \cdot & \cdot \cdot \cdot & \cdot \\ 0 & 0 & \ldots & \mu_n - \lambda \end{vmatrix} = \prod_{i=1}^{n} (\mu_i - \lambda),$$

car, après une transformation linéaire des indéterminées de matrice Q, le déterminant de la forme quadratique f se trouve multiplié par $|Q|^2$ (cf. § 28), et si Q est orthogonale, alors $|Q|^2 = 1$ (cf. § 35). La dernière égalité démontre le théorème.

On peut énoncer ce résultat sous la forme matricielle:

Quelle que soit la matrice orthogonale réduisant une matrice symétrique A à la forme diagonale, les éléments de la diagonale principale de la forme diagonale sont les racines caractéristiques de la matrice A, prises avec leurs ordres de multiplicité.

Procédé pratique pour trouver une application orthogonale réduisant une forme quadratique à ses axes principaux. Dans certains problèmes il ne suffit pas de connaître la forme canonique d'une forme quadratique, mais il s'agit également de trouver une application orthogonale qui réduit cette forme à la forme canonique. Il serait difficile de chercher cette application en s'appuyant sur la démonstration du théorème ci-dessus concernant la réduction des formes quadratiques. C'est pourquoi nous voulons indiquer un autre procédé. En fait, il faut un moyen pour trouver une matrice orthogonale Q telle qu'une matrice symétrique A donnée soit réductible par Q à la forme diagonale. Bien entendu, au lieu de Q on peut chercher son inverse Q^{-1}. D'après (2), la matrice Q^{-1} est la matrice de passage de la base e à la base f. Autrement dit, la matrice A étant celle d'une application symétrique φ rapportée à la base e et f_1, $f_2, \ldots, f_n$ étant une base orthonormale de n vecteurs propres de φ, la $i^{\text{ème}}$ ligne de la matrice Q^{-1} est la ligne des coordonnées du vecteur f_i, rapporté à la base e $(1 \leqslant i \leqslant n)$. Il reste à trouver la famille de vecteurs propres.

Soit λ_0 une racine caractéristique d'ordre de multiplicité k_0 de la matrice A. On sait du § 33 que l'ensemble des lignes des coordonnées des vecteurs propres de l'application φ, associés à la valeur propre λ_0, est le même que l'ensemble des solutions non nulles du système d'équations linéaires homogènes

$$(A-\lambda_0 E)X=0; \tag{3}$$

la matrice A étant symétrique, on peut la remplacer dans (3) par A'. Il résulte du théorème d'existence d'une matrice orthogonale réduisant une matrice symétrique A à la forme diagonale et du théorème d'unicité de la forme diagonale que le système (3) possède au moins k_0 solutions linéairement indépendantes. La famille de ces solutions peut être trouvée par les méthodes données au § 12 et orthonormalisée conformément au § 34.

Faisant dans (3) λ_0 successivement égal à toutes les racines caractéristiques distinctes de la matrice A, nous obtenons, compte tenu de ce que la somme des ordres de multiplicité des racines caractéristiques est égale à n, une famille de n vecteurs propres de l'application φ, donnés par leurs coordonnées, les vecteurs propres étant rapportés à la base e. Pour montrer que cette famille est bien la famille orthonormale cherchée, il reste à démontrer le *lemme* suivant:

Les vecteurs propres d'une application symétrique φ, *associés à des valeurs propres différentes, sont orthogonaux.*

En effet, soient

$$b\varphi=\lambda_1 b, \qquad c\varphi=\lambda_2 c,$$

avec $\lambda_1 \neq \lambda_2$. Etant donné que

$$(b\varphi, c)=(\lambda_1 b, c)=\lambda_1(b, c),$$
$$(b, c\varphi)=(b, \lambda_2 c)=\lambda_2(b, c),$$

on déduit de l'égalité

$$(b\varphi, c)=(b, c\varphi)$$

la relation

$$\lambda_1(b, c)=\lambda_2(b, c).$$

Compte tenu de ce que $\lambda_1 \neq \lambda_2$, il vient:

$$(b, c)=0,$$

ce qu'il fallait démontrer.

Exemple. Réduire la forme quadratique

$$f(x_1, x_2, x_3, x_4)=2x_1x_2+2x_1x_3-2x_1x_4-2x_2x_3+2x_2x_4+2x_3x_4$$

à ses axes principaux.

La matrice A de f est de la forme

$$A=\begin{pmatrix} 0 & 1 & 1 & -1 \\ 1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 \\ -1 & 1 & 1 & 0 \end{pmatrix}$$

Trouvons son polynôme caractéristique :

$$|A-\lambda E|=\begin{vmatrix} -\lambda & 1 & 1 & -1 \\ 1 & -\lambda & -1 & 1 \\ 1 & -1 & -\lambda & 1 \\ -1 & 1 & 1 & -\lambda \end{vmatrix}=(\lambda-1)^3(\lambda+3).$$

Ainsi, la matrice A a la racine caractéristique 1 d'ordre de multiplicité 3 et la racine caractéristique -3, simple. Par conséquent, nous connaissons déjà la forme canonique à laquelle la forme f est réductible par une application orthogonale :

$$f=y_1^2+y_2^2+y_3^2-3y_4^2.$$

Trouvons l'application orthogonale réduisant f. Le système d'équations linéaires homogènes (3) pour $\lambda_0=1$ prend la forme

$$\left\{\begin{array}{r} -x_1+x_2+x_3-x_4=0, \\ x_1-x_2-x_3+x_4=0, \\ x_1-x_2-x_3+x_4=0, \\ -x_1+x_2+x_3-x_4=0. \end{array}\right.$$

Le système étant de rang 1, on peut trouver trois solutions linéairement indépendantes, soit

$$b_1=(1,\ 1,\ 0,\ 0),$$
$$b_2=(1,\ 0,\ 1,\ 0),$$
$$b_3=(-1,\ 0,\ 0,\ 1).$$

Utilisant le procédé d'orthogonalisation, nous obtenons la famille de vecteurs

$$c_1=b_1=(1,\ 1,\ 0,\ 0),$$
$$c_2=-\frac{1}{2}c_1+b_2=\left(\frac{1}{2},\ -\frac{1}{2},\ 1,\ 0\right),$$
$$c_3=\frac{1}{2}c_1+\frac{1}{3}c_2+b_3=\left(-\frac{1}{3},\ \frac{1}{3},\ \frac{1}{3},\ 1\right).$$

D'autre part, faisant dans (3) $\lambda_0=-3$, nous obtenons le système d'équations linéaires homogènes

$$\left\{\begin{array}{r} 3x_1+x_2+x_3-x_4=0, \\ x_1+3x_2-x_3+x_4=0, \\ x_1-x_2+3x_3+x_4=0, \\ -x_1+x_2+x_3+3x_4=0. \end{array}\right.$$

Son rang est 3. La solution non nulle est donnée par le vecteur

$$c_4=(1,\ -1,\ -1,\ 1).$$

La famille des vecteurs c_1, c_2, c_3, c_4 est orthogonale. Passant aux vecteurs normés correspondants, nous obtenons la famille orthonormale des vecteurs

$$c_1'=\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0\right),$$

$$c_2'=\left(\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \sqrt{\frac{2}{3}}, 0\right),$$

$$c_3'=\left(-\frac{1}{2\sqrt{3}}, \frac{1}{2\sqrt{3}}, \frac{1}{2\sqrt{3}}, \frac{\sqrt{3}}{2}\right).$$

$$c_4'=\left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right).$$

Ainsi, la forme f est réductible à ses axes principaux par l'application orthogonale

$$y_1=\frac{1}{\sqrt{2}}x_1+\frac{1}{\sqrt{2}}x_2,$$

$$y_2=\frac{1}{\sqrt{6}}x_1-\frac{1}{\sqrt{6}}x_2+\sqrt{\frac{2}{3}}x_3,$$

$$y_3=-\frac{1}{2\sqrt{3}}x_1+\frac{1}{2\sqrt{3}}x_2+\frac{1}{2\sqrt{3}}x_3+\frac{\sqrt{3}}{2}x_4,$$

$$y_4=\frac{1}{2}x_1-\frac{1}{2}x_2-\frac{1}{2}x_3+\frac{1}{2}x_4.$$

Il faut noter que le choix de la famille de vecteurs propres linéairement indépendants, relatifs à une valeur propre multiple, est arbitraire, de sorte qu'il existe plusieurs applications orthogonales réduisant la forme f à la forme canonique. Nous n'en avons trouvé qu'une seule.

Couples de formes. Soit un couple de formes quadratiques réelles de n indéterminées: $f(x_1, x_2, \ldots, x_n)$ et $g(x_1, x_2, \ldots, x_n)$. Existe-t-il une transformation linéaire non dégénérée des indéterminées $x_1, x_2, \ldots, x_n$ telle que les deux formes f et g soient réductibles par cette transformation à la forme canonique?

La réponse est, en général, négative. Considérons, par exemple, le couple de formes

$$f(x_1, x_2)=x_1^2, \quad g(x_1, x_2)=x_1x_2.$$

Supposons qu'il existe une transformation linéaire non dégénérée

$$\left.\begin{aligned} x_1&=c_{11}y_1+c_{12}y_2,\\ x_2&=c_{21}y_1+c_{22}y_2,\end{aligned}\right\} \qquad (4)$$

réduisant les deux formes à la forme canonique. Pour que la transformation (4) réduise f à la forme canonique, il faut que l'un des coefficients c_{11} ou c_{12} soit nul, car, dans le cas contraire, on aurait le terme $2c_{11}c_{12}y_1y_2$. Echangeant, s'il le faut, les indices des y, on

peut supposer que $c_{12} = 0$; par conséquent, $c_{11} \neq 0$. Or, dans ce cas,

$$g(x_1, x_2) = c_{11}y_1(c_{21}y_1 + c_{22}y_2) = c_{11}c_{21}y_1^2 + c_{11}c_{22}y_1y_2.$$

La forme g devant être réduite par (4) à la forme canonique, on a nécessairement $c_{11}c_{22} = 0$, c'est-à-dire $c_{22} = 0$; c_{12} et c_{22} étant nuls, la transformation (4) est dégénérée.

La situation est toute différente si l'une des formes, soit $g(x_1, x_2, \ldots, x_n)$, est *définie positive* [1]. Notamment, le théorème suivant est vrai:

Soient f et g un couple de formes quadratiques réelles de n indéterminées, dont g est définie positive. Alors, il existe une transformation linéaire non dégénérée des indéterminées, réduisant simultanément g à la forme normale et f à la forme canonique.

Pour cela, réalisons d'abord la transformation linéaire non dégénérée des indéterminées $x_1, x_2, \ldots, x_n$, soit

$$X = TY,$$

qui réduit la forme définie positive g à la forme normale

$$g(x_1, x_2, \ldots, x_n) = y_1^2 + y_2^2 + \ldots + y_n^2.$$

Alors la forme f devient une forme quadratique, soit φ, des nouvelles indéterminées:

$$f(x_1, x_2, \ldots, x_n) = \varphi(y_1, y_2, \ldots, y_n).$$

Effectuons, ensuite, une transformation *orthogonale* des indéterminées $y_1, y_2, \ldots, y_n$,

$$Y = QZ,$$

qui réduit φ à ses axes principaux

$$\varphi(y_1, y_2, \ldots, y_n) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + \ldots + \lambda_n z_n^2.$$

Q (cf. § 35) associe à la somme des carrés des indéterminées $y_1, y_2, \ldots, y_n$ la somme des carrés des indéterminées $z_1, z_2, \ldots, z_n$. Finalement, nous obtenons

$$f(x_1, x_2, \ldots, x_n) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + \ldots + \lambda_n z_n^2,$$
$$g(x_1, x_2, \ldots, x_n) = z_1^2 + z_2^2 + \ldots + z_n^2,$$

de sorte que

$$X = (TQ)Z$$

est la transformation cherchée.

---

[1] Bien entendu, cette condition n'est pas nécessaire; par exemple, les formes $x_1^2 + x_2^2 - x_3^2$ et $x_1^2 - x_2^2 - x_3^2$, toutes deux canoniques, ne sont pas définies positives.

Chapitre IX | **CALCUL DES ZÉROS D'UN POLYNÔME**

§ 38*. Equations des deuxième, troisième et quatrième degrés

D'après le théorème fondamental démontré au § 23, tout polynôme de degré n à coefficients numériques possède exactement n zéros complexes. Néanmoins, aucune démonstration de ce théorème (ni celle donnée au § 23 ni toutes les autres connues jusqu'aujourd'hui) ne donne une méthode pratique de calcul des zéros ; ces démonstrations permettent seulement d'en établir l'existence.

Naturellement, on a d'abord essayé d'établir des formules analogues à celle donnant les racines d'une équation du deuxième degré ; le lecteur connaît cette formule du cours d'algèbre élémentaire, lorsque les coefficients de l'équation sont réels. Nous allons montrer qu'elle reste valable dans le cas des équations du deuxième degré à coefficients complexes et que des formules analogues (mais plus compliquées) peuvent être établies pour les équations du troisième et du quatrième degré.

Equations du deuxième degré. Soit une équation du deuxième degré à coefficients complexes

$$x^2+px+q=0.$$

On peut supposer, sans restreindre la généralité, que le coefficient du terme du deuxième degré en x est égal à l'unité. On peut récrire cette équation sous la forme

$$\left(x+\frac{p}{2}\right)^2+\left(q-\frac{p^2}{4}\right)=0.$$

On sait que les valeurs de la racine carrée du nombre complexe $\frac{p^2}{4}-q$ sont des nombres complexes. La racine carrée ayant deux valeurs opposées, on peut les noter $\pm\sqrt{\frac{p^2}{4}-q}$. Ainsi

$$x+\frac{p}{2}=\pm\sqrt{\frac{p^2}{4}-q}.$$

c'est-à-dire les racines de l'équation donnée peuvent être calculées selon la formule usuelle:

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Exemple. Résoudre l'équation

$$x^2 - 3x + (3 - i) = 0.$$

Appliquant la formule établie ci-dessus, il vient:

$$x = \frac{3}{2} \pm \sqrt{\frac{9}{4} - (3 - i)} = \frac{3}{2} \pm \frac{1}{2}\sqrt{-3 + 4i}.$$

Au moyen des méthodes du § 19, on trouve:

$$\sqrt{-3 + 4i} = \pm (1 + 2i),$$

de sorte que

$$x_1 = 2 + i, \quad x_2 = 1 - i.$$

Equations du troisième degré. A la différence du cas des équations du deuxième degré nous n'avons pas jusqu'à maintenant de méthodes pour la résolution des équations du troisième degré, même lorsque les coefficients sont réels. Nous allons établir pour les équations du troisième degré une formule analogue à la formule qui donne les racines des équations du deuxième degré; en outre, nous supposons, dès le début, que les coefficients des équations sont des nombres complexes quelconques.

Soit une équation du troisième degré à coefficients complexes

$$y^3 + ay^2 + by + c = 0. \qquad (1)$$

Remplaçant dans (1) l'inconnue y par une nouvelle inconnue x, liée à y par la relation

$$y = x - \frac{a}{3}, \qquad (2)$$

il est facile de vérifier que nous obtenons pour l'inconnue x une équation où le terme en x^2 disparaît, c'est-à-dire une équation de la forme

$$x^3 + px + q = 0. \qquad (3)$$

Calculant les racines de l'équation (3), nous pouvons, d'après (2), trouver celles de l'équation (1). Donc, il reste à trouver une méthode de résolution de l'équation du troisième degré « non complète » à coefficients complexes (3).

D'après le théorème fondamental, l'équation (3) possède trois racines complexes. Soit x_0 l'une de ces racines. Introduisons une inconnue auxiliaire u et considérons le polynôme

$$f(u) = u^2 - x_0 u - \frac{p}{3}.$$

Ses coefficients étant des nombres complexes, cette équation possède deux racines complexes α et β; en outre, selon les formules de Viète on a

$$\alpha+\beta=x_0, \tag{4}$$

$$\alpha\beta=-\frac{p}{3}. \tag{5}$$

Portant dans (3) l'expression (4) de la racine x_0, nous obtenons:

$$(\alpha+\beta)^3+p(\alpha+\beta)+q=0$$

ou encore

$$\alpha^3+\beta^3+(3\alpha\beta+p)(\alpha+\beta)+q=0.$$

Or, il s'ensuit de (5) que $3\alpha\beta+p=0$, de sorte que l'on a:

$$\alpha^3+\beta^3=-q. \tag{6}$$

D'autre part, il découle de (5)

$$\alpha^3\beta^3=-\frac{p^3}{27}. \tag{7}$$

Les égalités (6) et (7) montrent que les nombres α^3 et β^3 sont les racines de l'équation du deuxième degré à coefficients complexes

$$z^2+qz-\frac{p^3}{27}=0. \tag{8}$$

Résolvant l'équation (8), il vient:

$$z=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}},$$

d'où l'on a[1]

$$\alpha=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},\quad \beta=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}. \tag{9}$$

Nous sommes conduits à la relation, dite *formule de Cardan*, qui exprime les racines de l'équation (3) par les coefficients au moyen de racines carrées et cubiques:

$$x_0=\alpha+\beta=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

La racine cubique d'un nombre complexe a trois valeurs com plexes, de sorte que les formules (9) donnent trois valeurs pour α et

[1] Les nombres α et β intervenant de manière symétrique dans les égalités (6) et (7) et dans l'expression (4) de x_0, on peut donc choisir, sans différence aucune, pour α^3 (respectivement pour β^3) la première ou la seconde racine de l'équation (8).

autant de valeurs pour β. Cependant, si l'on veut appliquer la formule de Cardan, on ne peut pas prendre les valeurs de α indépendamment de celles de β : pour toute valeur de α il faut prendre la valeur de β qui vérifie la condition (5).

Soit α_1 l'une des trois valeurs de α, données par la formule (9). On a montré au § 19 que les deux autres valeurs de α s'obtiennent en multipliant α_1 par les racines cubiques de l'unité ε et ε^2 :

$$\alpha_2 = \alpha_1\varepsilon, \qquad \alpha_3 = \alpha_1\varepsilon^2.$$

Désignons par β_1 celle des trois valeurs de β, données par la formule (9), qui correspond à la valeur α_1 de α, d'après la relation (5), c'est-à-dire β_1 est la valeur de β telle que l'on ait : $\alpha_1\beta_1 = -\frac{p}{3}$. Les deux autres valeurs de β sont

$$\beta_2 = \beta_1\varepsilon, \qquad \beta_3 = \beta_1\varepsilon^2.$$

Vu que $\varepsilon^3 = 1$ et que

$$\alpha_2\beta_3 = \alpha_1\varepsilon \cdot \beta_1\varepsilon^2 = \alpha_1\beta_1\varepsilon^3 = \alpha_1\beta_1 = -\frac{p}{3},$$

à la valeur α_2 de α correspond la valeur β_3 de β ; d'une manière analogue, à la valeur α_3 correspond la valeur β_2. Ainsi, les trois racines de l'équation (3) peuvent être écrites de la manière suivante :

$$\left.\begin{aligned} x_1 &= \alpha_1 + \beta_1, \\ x_2 &= \alpha_2 + \beta_3 = \alpha_1\varepsilon + \beta_1\varepsilon^2, \\ x_3 &= \alpha_3 + \beta_2 = \alpha_1\varepsilon^2 + \beta_1\varepsilon. \end{aligned}\right\} \qquad (10)$$

Equations du troisième degré à coefficients réels. Voyons ce qu'on peut dire des racines d'une équation du troisième degré non complète

$$x^3 + px + q = 0, \qquad (11)$$

si ses coefficients sont réels. Dans ce cas, le rôle du signe de l'expression $\frac{q^2}{4} + \frac{p^3}{27}$, se trouvant sous la racine carrée dans la formule de Cardan, se révèle très important. Remarquons que ce signe est opposé à celui de l'expression

$$D = -4p^3 - 27q^2 = -108\left(\frac{q^2}{4} + \frac{p^3}{27}\right),$$

dite *discriminant* de l'équation (11) (cf. § 54) ; les énoncés qui suivront utiliseront le signe du discriminant.

1) Soit $D < 0$. Dans ce cas, le même nombre réel positif se trouve sous les racines carrées dans la formule de Cardan, de sorte que l'on extrait les racines cubiques des nombres *réels*. Or, la racine cubique

d'un nombre réel a une valeur réelle et deux valeurs conjuguées complexes. Soit α_1 la valeur réelle de α; alors, la valeur β_1 de β, qui correspond à α_1 d'après la formule (5), est également un nombre réel, car p est réel. Ainsi, la racine $x_1 = \alpha_1 + \beta_1$ de l'équation (11) est réelle. On trouve les deux autres racines, en remplaçant dans les formules (10) de ce paragraphe les racines cubiques de l'unité $\varepsilon = \varepsilon_1$ et $\varepsilon^2 = \varepsilon_2$ par leurs expressions (7) du § 19:

$$x_2 = \alpha_1\varepsilon + \beta_1\varepsilon^2 = \alpha_1\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) + \beta_1\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) =$$
$$= -\frac{\alpha_1+\beta_1}{2} + i\sqrt{3}\,\frac{\alpha_1-\beta_1}{2},$$
$$x_3 = \alpha_1\varepsilon^2 + \beta_1\varepsilon = \alpha_1\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) + \beta_1\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) =$$
$$= -\frac{\alpha_1+\beta_1}{2} - i\sqrt{3}\,\frac{\alpha_1-\beta_1}{2};$$

les nombres α_1 et β_1 étant réels, les racines x_2 et x_3 sont des nombres conjugués complexes; en outre, le coefficient de la partie imaginaire de x_2 et de x_3 est non nul, car $\alpha_1 \neq \beta_1$ (α_1 et β_1 sont des valeurs des racines cubiques distinctes).

Ainsi, *si $D < 0$, alors l'équation* (11) *a une racine réelle et deux racines conjuguées complexes.*

2) Soit $D = 0$. Dans ce cas,

$$\alpha = \sqrt[3]{-\frac{q}{2}}, \qquad \beta = \sqrt[3]{-\frac{q}{2}}.$$

Soit α_1 la valeur réelle de la racine cubique α. En vertu de (5), β_1 est également un nombre réel; en outre, $\alpha_1 = \beta_1$. Remplaçant dans les formules (10) β_1 par α_1 et utilisant l'égalité évidente $\varepsilon + \varepsilon^2 = -1$, il vient:

$$x_1 = 2\alpha_1,\ x_2 = \alpha_1(\varepsilon + \varepsilon^2) = -\alpha_1,\ x_3 = \alpha_1(\varepsilon^2 + \varepsilon) = -\alpha_1.$$

Ainsi, *si $D = 0$, alors l'équation* (11) *a ses racines réelles dont deux coïncident.*

3) Enfin, soit $D > 0$. Dans ce cas, on a le même nombre réel négatif sous les racines carrées dans la formule de Cardan, de sorte que les racines cubiques doivent être extraites des nombres conjugués complexes. Ainsi, toutes les valeurs de α et β sont maintenant des nombres complexes. Or, parmi les racines de l'équation (11) l'une au moins est réelle. Supposons que la racine

$$x_1 = \alpha_0 + \beta_0$$

soit réelle. La somme et le produit des nombres α_0 et β_0 étant réels $\left(\text{rappelons que } \alpha_0\beta_0 = -\frac{p}{3}\right)$, il s'ensuit que les nombres α_0 et β_0

sont conjugués, en tant que racines d'une équation du deuxième degré à coefficients réels. Alors, les couples de nombres $\alpha_0\varepsilon$, $\beta_0\varepsilon^2$ et $\alpha_0\varepsilon^2$, $\beta_0\varepsilon$ sont également conjugués, d'où il découle que les racines de l'équation (11)

$$x_2 = \alpha_0\varepsilon + \beta_0\varepsilon^2, \qquad x_3 = \alpha_0\varepsilon^2 + \beta_0\varepsilon$$

sont aussi des nombres réels.

Ainsi, dans ce cas, toutes les racines de l'équation (11) sont réelles; en outre, il est facile de montrer qu'elles sont distinctes. En effet, supposant le contraire, on peut choisir la racine x_1 de manière que $x_2 = x_3$, d'où l'on a

$$\alpha_0(\varepsilon - \varepsilon^2) = \beta_0(\varepsilon - \varepsilon^2),$$

c'est-à-dire $\alpha_0 = \beta_0$; or, cela est impossible.

Ainsi, *si $D > 0$, alors l'équation* (11) *a trois racines réelles distinctes.*

Le dernier résultat montre que l'intérêt pratique de la formule de Cardan est relativement petit. En effet, bien que les racines de l'équation (11) à coefficients réels soient réelles pour $D > 0$, leur calcul selon la formule de Cardan nécessite l'extraction de racines cubiques de nombres complexes, et nous ne savons le faire qu'en passant à la forme trigonométrique de ces nombres. Ainsi, l'expression des zéros d'un polynôme du troisième degré à coefficients réels au moyen de racines carrées et cubiques n'a pas de valeur pratique. Utilisant certaines méthodes (dépassant le cadre de notre livre) on pourrait montrer que dans le cas considéré les racines de l'équation (11) ne peuvent point être exprimées par les coefficients au moyen de racines de nombres réels. Ce cas de la résolution de l'équation (11) est dit *irréductible* (ne pas confondre avec l'irréductibilité des polynômes !).

Exemples. 1. Résoudre l'équation

$$y^3 + 3y^2 - 3y - 14 = 0.$$

Posant $y = x - 1$, nous trouvons l'équation

$$x^3 - 6x - 9 = 0. \tag{12}$$

Ici $p = -6$, $q = -9$, de sorte que

$$\frac{q^2}{4} + \frac{p^3}{27} = \frac{49}{4} > 0,$$

c'est-à-dire l'équation (12) a une racine réelle et deux racines conjuguées complexes. D'après (9) on a $\alpha = \sqrt[3]{\frac{9}{2} + \frac{7}{2}} = \sqrt[3]{8}$, $\beta = \sqrt[3]{\frac{9}{2} - \frac{7}{2}} = \sqrt[3]{1}$. Ainsi, $\alpha_1 = 2$, $\beta_1 = 1$, c'est-à-dire $x_1 = 3$. Les deux autres racines s'obtiennent par les formules (10) : $x_2 = -\frac{3}{2} + i\frac{\sqrt{3}}{2}$, $x_3 = -\frac{3}{2} - i\frac{\sqrt{3}}{2}$

Il en résulte que les racines de l'équation donnée sont

$$y_1 = 2, \quad y_2 = -\frac{5}{2} + i\,\frac{\sqrt{3}}{2}, \quad y_3 = -\frac{5}{2} - i\,\frac{\sqrt{3}}{2}.$$

2. Résoudre l'équation

$$x^3 - 12x + 16 = 0.$$

Ici $p = -12$, $q = 16$, de sorte que l'on a

$$\frac{q^2}{4} + \frac{p^3}{27} = 0.$$

Il en découle que $\alpha = \sqrt[3]{-8}$, c'est-à-dire $\alpha_1 = -2$. Par conséquent,

$$x_1 = -4, \quad x_2 = x_3 = 2.$$

3. Résoudre l'équation

$$x^3 - 19x + 30 = 0.$$

Ici $p = -19$, $q = 30$, de sorte que

$$\frac{q^2}{4} + \frac{p^3}{27} = -\frac{784}{27} < 0.$$

Ainsi, si l'on veut rester dans le domaine des nombres réels, la formule de Cardan n'est pas valable pour cette équation, bien que ses racines soient les nombres réels 2, 3 et -5.

Equations du quatrième degré. Le calcul des racines d'une équation du quatrième degré à coefficients complexes

$$y^4 + ay^3 + by^2 + cy + d = 0 \tag{13}$$

se ramène à la résolution d'une équation auxiliaire du troisième degré. On réalise cette réduction par la méthode suivante due à Ferrari.

D'abord, posant $y = x - \frac{a}{4}$, on ramène l'équation (13) à la forme

$$x^4 + px^2 + qx + r = 0. \tag{14}$$

Ensuite, on transforme le premier membre de cette équation en introduisant un paramètre auxiliaire α de la manière suivante :

$$x^4 + px^2 + qx + r = \left(x^2 + \frac{p}{2} + \alpha\right)^2 + qx + r - \frac{p^2}{4} - \alpha^2 - 2\alpha x^2 - p\alpha$$

ou encore

$$\left(x^2 + \frac{p}{2} + \alpha\right)^2 - \left[2\alpha x^2 - qx + \left(\alpha^2 + p\alpha - r + \frac{p^2}{4}\right)\right] = 0. \tag{15}$$

Choisissons α de manière que le polynôme entre les crochets soit le carré d'un polynôme du premier degré. Pour cela, ce polynôme

doit avoir un zéro double, c'est-à-dire on doit avoir l'égalité

$$q^2-4\cdot 2\alpha\left(\alpha^2+p\alpha-r+\frac{p^2}{4}\right)=0. \qquad (16)$$

L'égalité (16) est une équation du troisième degré à coefficients complexes par rapport à α. On sait que cette équation a trois racines complexes. On en choisit une, soit α_0; d'après la formule de Cardan, α_0 s'exprime par les coefficients de l'équation (16) et, par conséquent, par les coefficients de l'équation (14), au moyen de racines troisièmes au plus.

α étant choisi de cette manière, le polynôme entre les crochets dans (15) a le zéro double $\frac{q}{4\alpha_0}$, de sorte que l'équation (15) prend la forme

$$\left(x^2+\frac{p}{2}+\alpha_0\right)^2-2\alpha_0\left(x-\frac{q}{4\alpha_0}\right)^2=0,$$

c'est-à-dire elle se décompose en deux équations du deuxième degré

$$\left.\begin{aligned} x^2-\sqrt{2\alpha_0}\,x+\left(\frac{p}{2}+\alpha_0+\frac{q}{2\sqrt{2\alpha_0}}\right)=0,\\ x^2+\sqrt{2\alpha_0}\,x+\left(\frac{p}{2}+\alpha_0-\frac{q}{2\sqrt{2\alpha_0}}\right)=0.\end{aligned}\right\} \qquad (17)$$

Nous avons été amenés en partant de l'équation (14) aux équations (17) à l'aide d'un certain nombre de transformations réversibles; par conséquent, les racines des équations (17) sont celles de l'équation (14). En outre, il est facile de voir que les racines de l'équation (14) s'expriment par les coefficients au moyen de radicaux. Nous ne donnerons pas ici les formules correspondantes, car elles sont trop encombrantes et n'ont aucune utilité pratique; nous n'étudierons pas non plus le cas particulier où les coefficients de l'équation (14) sont réels.

Remarques sur les équations de degrés supérieurs. Les méthodes de résolution des équations du deuxième degré étaient déjà connues des anciens Grecs, et la découverte des méthodes de résolution des équations du troisième et du quatrième degré, exposées ci-dessus, remonte au XVI[e] siècle. Puis suivirent presque trois siècles de vains efforts pour faire le pas suivant, c'est-à-dire trouver des formules qui donneraient les racines d'une équation du cinquième degré en fonction des coefficients au moyen de radicaux (les équations étant à coefficients *littéraux* quelconques). Il fallut le résultat d'Abel, établi dans les années vingt du siècle dernier, pour mettre fin à ces tentatives; d'après ce résultat il n'existe pas de telles formules pour les racines d'une équation de degré n, lorsque $n \geqslant 5$.

Le résultat d'Abel n'excluait pourtant pas la possibilité pour tout polynôme concret à coefficients numériques de trouver ses zéros en fonction des coefficients au moyen des racines n^{emes}; autrement dit; ce résultat n'écartait pas la conjecture que toute équation concrète soit résoluble par radicaux. Le problème de la résolution par radicaux des équations de degré n a été étudié en détail par Galois dans les années trente du siècle dernier. Il s'est révélé que pour tout n, à partir de $n = 5$, on peut indiquer des équations de degré n à coefficients numériques (même à coefficients entiers) qui ne peuvent pas être résolues par radicaux. Ainsi, l'équation

$$x^5 - 4x - 2 = 0$$

est une équation de ce genre.

Les recherches de Galois ont déterminé tout le développement ultérieur de l'algèbre. Néanmoins, l'exposé de la théorie de Galois ne fera pas l'objet de notre cours.

§ 39. Limites des zéros

Nous savons qu'il n'existe pas de méthode permettant de trouver les expressions exactes des zéros des polynômes à coefficients numériques. Néanmoins, les différents problèmes de mécanique, de physique, ainsi que des problèmes de technique se ramènent au calcul des zéros de polynômes; en outre, ces polynômes ont souvent des degrés assez élevés. C'est ce genre de problèmes qui ont stimulé de nombreuses recherches ayant pour objet l'étude de certaines propriétés des zéros d'un polynôme à coefficients numériques sans être obligé de calculer ces zéros. Par exemple, on a étudié le problème de répartition des zéros dans le plan complexe (notamment, les conditions garantissant que les zéros d'un polynôme se trouvent à l'intérieur d'un cercle de rayon unité, c'est-à-dire les conditions pour que les modules des zéros soient inférieurs à l'unité ou, encore, les conditions pour que les zéros d'un polynôme appartiennent au demi-plan gauche, c'est-à-dire qu'ils aient les parties réelles négatives, etc.). Pour les polynômes à coefficients réels on a élaboré des méthodes permettant de déterminer le nombre de zéros réels, ainsi que des méthodes qui permettent de les localiser, etc. Enfin, de nombreuses recherches ont été consacrées aux calculs approchés des zéros: dans les applications techniques, il suffit, en général, de connaître les valeurs approchées des zéros avec une précision donnée à l'avance, de sorte que si, par exemple, nous avions les expressions des zéros au moyen de radicaux, nous serions obligés de remplacer ceux-ci par des valeurs approchées avec une précision satisfaisante.

Tous ces problèmes étaient, dans le temps, l'objet d'étude de l'algèbre supérieure. Notre cours renferme seulement un petit nombre de résultats se rapportant à ces problèmes ; en outre, tenant compte des applications, nous nous limitons au cas des polynômes à coefficients réels et au problème de calcul de leurs zéros réels, ne sortant que rarement du cadre de ces problèmes. Le polynôme à coefficients réels $f(x)$ sera considéré comme une fonction réelle (continue) de la variable réelle x; en outre, nous utiliserons les méthodes d'analyse partout où cela se révélera efficace.

Il est utile de commencer l'étude des zéros réels d'un polynôme à coefficients réels $f(x)$, en considérant le graphe de $f(x)$. Il est clair que les *zéros réels du polynôme $f(x)$ sont les abscisses des points d'intersection du graphe de $f(x)$ avec l'axe des abscisses; $f(x)$ n'a pas d'autres zéros réels.*

Considérons, par exemple, le polynôme du cinquième degré

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3.$$

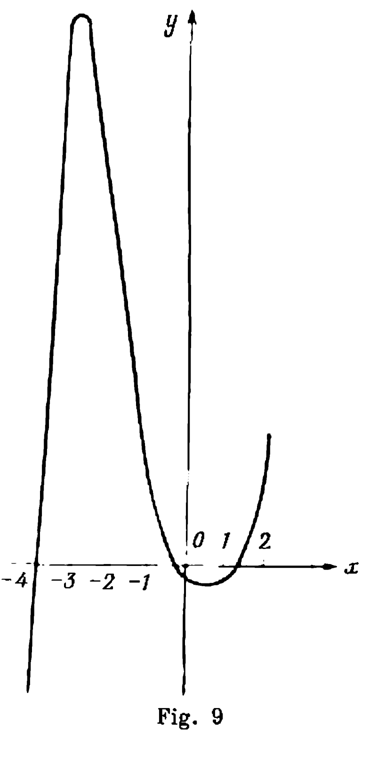


Fig. 9

D'après les résultats du § 24 sur les zéros des polynômes, on peut affirmer que $h(x)$ a au moins un zéro réel, car $f(x)$ est de degré impair ; en outre, si le nombre de zéros réels de $h(x)$ est supérieur à un, alors ce nombre est égal a trois ou bien à cinq, car les zéros complexes sont conjugués deux à deux.

Le graphe du polynôme $h(x)$ permet d'obtenir plus de renseignements sur ses zéros. Calculant les valeurs de $h(x)$ pour x entiers (par exemple, au moyen du procédé de Hörner), traçons le graphe en question (fig. 9) [1].

[1] L'échelle de l'axe des y est, sur la figure 9, dix fois plus petite que celle de l'axe des x.

x	$h(x)$	x	$h(x)$
.	.	-1	18
.	.	0	-3
.	.	1	-4
-4	-39	2	39
-3	144	.	.
-2	83	.	.

On voit que le polynôme $h(x)$ possède, en tout cas, trois zéros réels dont un positif, α_1, et deux négatifs, α_2 et α_3; en outre,

$$1 < \alpha_1 < 2, \qquad -1 < \alpha_2 < 0,$$
$$-4 < \alpha_3 < -3.$$

L'information sur les zéros (réels) d'un polynôme, fournie par le graphe, est pratiquement assez satisfaisante. Néanmoins, chaque fois il reste des doutes concernant l'existence d'autres zéros réels. Ainsi, dans l'exemple considéré ci-dessus nous n'avons pas démontré qu'il n'existait pas de zéros de $h(x)$ à droite du point $x = 2$ et à gauche du point $x = -4$. De plus, n'ayant pas considéré les valeurs non entières de x, on peut admettre que le graphe tracé sur la fig. 9 ne correspond pas tout à fait au véritable comportement de la fonction $h(x)$, notamment il ne prend pas en considération les oscillations plus petites de $h(x)$ et, pour cette raison, il est possible qu'on perde de vue certains zéros de cette fonction.

Il est vrai qu'on aurait pu, en traçant le graphe de $h(x)$, prendre les valeurs de $h(x)$ qui correspondent non seulement aux valeurs entières de x, mais aussi aux valeurs de la variable indépendante qui en diffèrent de 0,1 ou, encore, de 0,01. Mais cela ne ferait que compliquer les calculs, sans faire disparaître les doutes évoqués ci-dessus. D'autre part, on pourrait, utilisant les méthodes d'analyse, étudier le comportement de la fonction $h(x)$ en déterminant ses points extrémaux et comparer ainsi notre graphe avec l'allure véritable de $h(x)$; or, cela conduit au problème du calcul des zéros de la dérivée $h'(x)$, c'est-à-dire encore au problème qui nous préoccupe.

Il en résulte la nécessité de trouver des méthodes plus efficaces de calcul des limites des zéros des polynômes à coefficients réels, ainsi que des méthodes permettant de déterminer le nombre de ces zéros. Nous allons aborder le problème de calcul des limites des zéros réels; le problème de détermination du nombre de zéros réels sera étudié aux paragraphes suivants.

La démonstration du lemme du module du terme principal (cf. § 23) permet déjà d'établir certaines limites pour les modules des zéros

d'un polynôme. En effet, posant $k = 1$ dans (3) du § 23, nous obtenons, pour

$$|x| \geqslant 1 + \frac{A}{|a_0|}, \tag{1}$$

où a_0 est le coefficient du terme principal et A le maximum des modules des autres coefficients, que le module du terme principal est strictement supérieur au module de la somme de tous les autres termes, de sorte qu'aucune valeur de x, vérifiant (1), ne peut être zéro de ce polynôme.

Ainsi, *quel que soit le polynôme $f(x)$ à coefficients numériques, le nombre $1 + \frac{A}{|a_0|}$ est une borne supérieure des modules des zéros réels et complexes de $f(x)$*. Ainsi, pour le polynôme $h(x)$ considéré ci-dessus on a : $a_0 = 1$, $A = 8$, de sorte que le nombre 9 est une borne supérieure des modules des racines de $h(x)$.

Néanmoins, la borne supérieure (1) étant trop grossière, surtout lorsqu'on ne cherche que les zéros réels, nous allons donner d'autres méthodes, plus précises. En outre, il ne faut pas oublier que si l'on donne des limites entre lesquelles les zéros réels peuvent être compris, *cela ne veut nullement dire que ces zéros existent réellement.*

Montrons d'abord qu'*il suffit de trouver une borne supérieure des zéros positifs d'un polynôme.* En effet, soient un polynôme $f(x)$ de degré n et N_0 une borne supérieure des zéros positifs de $f(x)$. Considérons les polynômes

$$\varphi_1(x) = x^n f\left(\frac{1}{x}\right)$$
$$\varphi_2(x) = f(-x),$$
$$\varphi_3(x) = x^n f\left(-\frac{1}{x}\right).$$

Soient N_1, N_2, N_3 des bornes supérieures respectives des zéros positifs de ces polynômes. Alors *le nombre $\frac{1}{N_1}$ est une borne inférieure des zéros positifs du polynôme $f(x)$*; en effet, α étant un zéro positif de $f(x)$, le nombre $\frac{1}{\alpha}$ est un zéro positif de $\varphi_1(x)$ et l'inégalité $\frac{1}{\alpha} < N_1$ entraîne $\alpha > \frac{1}{N_1}$. De même, *les nombres $-N_2$ et $-\frac{1}{N_3}$ sont respectivement des bornes inférieure et supérieure des zéros négatifs du polynôme $f(x)$*. Ainsi, tout zéro positif du polynôme $f(x)$ vérifie l'inégalité $\frac{1}{N_1} < x < N_0$, de même que tout zéro négatif de $f(x)$ satisfait à l'inégalité

$$-N_2 < x < -\frac{1}{N_3}$$

On peut appliquer la méthode suivante pour trouver une borne supérieure des zéros positifs. Soit un polynôme à coefficients réels

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n;$$

on suppose en outre que $a_0 > 0$. Soit ensuite a_k, $k \geqslant 1$, le premier coefficient négatif de $f(x)$; si tous les coefficients du polynôme $f(x)$ étaient positifs, alors $f(x)$ ne pourrait pas avoir de zéros positifs. Enfin, notons par B la plus grande des valeurs absolues des coefficients négatifs de $f(x)$. Alors *le nombre*

$$1 + \sqrt[k]{\frac{B}{a_0}}$$

est une borne supérieure des zéros positifs du polynôme $f(x)$.

En effet, soit $x > 1$; remplaçant dans l'expression de $f(x)$ les coefficients $a_1, a_2, \ldots, a_{k-1}$ par le nombre zéro et les coefficients $a_k, a_{k+1}, \ldots, a_n$ par le nombre $-B$, la valeur de $f(x)$ n'en devient que plus petite,

$$f(x) \geqslant a_0x^n - B(x^{n-k} + x^{n-k-1} + \ldots + x + 1) =$$
$$= a_0x^n - B\frac{x^{n-k+1} - 1}{x-1},$$

de sorte que, en vertu de $x > 1$, on a

$$f(x) > a_0x^n - \frac{Bx^{n-k+1}}{x-1} = \frac{x^{n-k+1}}{x-1}\left[a_0x^{k-1}(x-1) - B\right] \tag{2}$$

Si

$$x > 1 + \sqrt[k]{\frac{B}{a_0}}, \tag{3}$$

alors l'expression entre les crochets dans la formule (2) est strictement positive, vu que pour $x > 1$ on a l'inégalité

$$a_0x^{k-1}(x-1) - B \geqslant a_0(x-1)^k - B;$$

par conséquent, en vertu de (2), la valeur de $f(x)$ est strictement positive. Ainsi, aucune valeur de x vérifiant l'inégalité (3) ne peut être zéro de $f(x)$, ce qu'il fallait démontrer.

Pour le polynôme $h(x)$ considéré ci-dessus on a : $k = 2$ et $B = 7$, et notre méthode donne le nombre $1 + \sqrt{7}$ pour borne supérieure des zéros positifs de $h(x)$; on peut le remplacer par le nombre 4 qui est le plus petit nombre entier majorant $1 + \sqrt{7}$.

Parmi les nombreuses autres méthodes de calcul de bornes supérieures des zéros positifs nous donnerons encore celle due à *Newton*. Quoique cette méthode soit plus laborieuse que celle exposée ci-dessus, elle donne d'habitude de très bons résultats.

Soit un polynôme à coefficients réels $f(x)$ dont le coefficient du terme principal a_0 est positif. *Si le polynôme $f(x)$ et ses dérivées $f'(x)$, $f''(x)$, ..., $f^{(n)}(x)$ sont positifs pour $x = c$, alors le nombre c est une borne supérieure des zéros positifs.*

En effet, d'après la formule de Taylor (cf. § 23) on a

$$f(x)=f(c)+(x-c)f'(c)+(x-c)^2\frac{f''(c)}{2!}+\dots$$
$$\dots+(x-c)^n\frac{f^{(n)}(c)}{n!}.$$

On voit que le second membre est strictement positif pour $x \geqslant c$, c'est-à-dire aucune valeur de x vérifiant l'inégalité $x \geqslant c$ ne peut être zéro de $f(x)$.

Il est utile de procéder de la manière suivante en calculant le nombre correspondant c pour un polynôme donné $f(x)$. La dérivée $f^{(n)}(x) = n!a_0$ étant un nombre positif, le polynôme $f^{(n-1)}(x)$ est une fonction croissante de x. Donc, il existe un nombre c_1 tel que la dérivée $f^{(n-1)}(x)$ est positive pour $x \geqslant c_1$. Il en résulte que la dérivée $f^{(n-2)}(x)$ est une fonction croissante de x pour $x \geqslant c_1$, de sorte qu'il existe un nombre c_2, $c_2 \geqslant c_1$, tel que la dérivée $f^{(n-2)}(x)$ est positive pour $x \geqslant c_2$. Continuant ce processus, ou trouvera, finalement, le nombre c.

Appliquons la méthode de Newton au polynôme $h(x)$ considéré ci-dessus. On a

$$\begin{aligned}
h(x) &= x^5+2x^4-5x^3+8x^2-7x-3,\\
h'(x) &= 5x^4+8x^3-15x^2+16x-7,\\
h''(x) &= 20x^3+24x^2-30x+16,\\
h'''(x) &= 60x^2+48x-30,\\
h^{\mathrm{IV}}(x) &= 120x+48,\\
h^{\mathrm{V}}(x) &= 120.
\end{aligned}$$

Il est facile de vérifier (utilisant, par exemple, le procédé de Hörner) que tous ces polynômes sont positifs pour $x = 2$. Ainsi, le nombre 2 est une borne supérieure des zéros positifs du polynôme $h(x)$; c'est là un résultat beaucoup plus précis que ceux obtenus ci-dessus par d'autres méthodes.

Pour calculer une borne inférieure des zéros négatifs de $h(x)$ considérons le polynôme $\varphi_2(x) = -h(-x)$ [1]. On a

$$\begin{aligned}
\varphi_2(x) &= x^5-2x^4-5x^3-8x^2-7x+3,\\
\varphi_2'(x) &= 5x^4-8x^3-15x^2-16x-7,\\
\varphi_2''(x) &= 20x^3-24x^2-30x-16,\\
\varphi_2'''(x) &= 60x^2-48x-30,\\
\varphi_2^{\mathrm{IV}}(x) &= 120x-48,\\
\varphi_2^{\mathrm{V}}(x) &= 120;
\end{aligned}$$

[1] On prend $-h(-x)$ au lieu de $h(-x)$, car le coefficient du terme principal doit être positif afin que l'on puisse appliquer la méthode de Newton. Bien entendu, cela ne modifie pas les zéros du polynôme $\varphi_2(x)$.

tous ces polynômes étant positifs pour $x = 4$, ce qui est facile de vérifier, le nombre 4 est une borne supérieure des zéros positifs de $\varphi_2(x)$, de sorte que le nombre -4 est une borne inférieure des zéros négatifs de $h(x)$.

Enfin, considérant les polynômes

$$\varphi_1(x) = -x^5 h\left(\frac{1}{x}\right) = 3x^5 + 7x^4 - 8x^3 + 5x^2 - 2x - 1,$$

$$\varphi_3(x) = -x^5 h\left(-\frac{1}{x}\right) = 3x^5 - 7x^4 - 8x^3 - 5x^2 - 2x + 1,$$

on trouve des bornes supérieures de leurs zéros positifs qui sont, respectivement, les nombres 1 et 4 en appliquant la méthode de Newton. Par conséquent, le nombre $\frac{1}{1} = 1$ est une borne inférieure des zéros positifs de $h(x)$ et le nombre $-\frac{1}{4}$ une borne supérieure des zéros négatifs de $h(x)$.

Ainsi, les zéros positifs de $h(x)$ sont compris entre les nombres 1 et 2, et ses zéros négatifs se trouvent entre les nombres -4 et $-\frac{1}{4}$. Ce résultat est bien en accord avec l'information fournie par le graphe de $h(x)$.

§ 40. Théorème de Sturm

Nous passons maintenant au problème de la détermination du *nombre des zéros réels d'un polynôme $f(x)$ à coefficients réels.* En outre, on s'intéressera non seulement au problème du calcul du nombre total des zéros réels de $f(x)$, mais aussi à celui de la détermination du nombre de zéros positifs, négatifs et, plus généralement, de zéros compris entre des nombres donnés a et b. Il existe plusieurs méthodes de calcul du nombre exact des zéros d'un polynôme; elles sont toutes assez laborieuses; parmi ces méthodes celle de *Sturm* est la plus commode et nous allons l'exposer.

Introduisons d'abord une définition qu'on utilisera également dans le paragraphe suivant.

Soit une suite finie ordonnée de nombres réels non nuls, par exemple,

$$1,\ 3,\ -2,\ 1,\ -4,\ -8,\ -3,\ 4,\ 1. \tag{1}$$

Ecrivons successivement les signes qui précèdent ces nombres

$$+,\ +,\ -,\ +,\ -,\ -,\ -,\ +,\ +. \tag{2}$$

Nous constatons que dans la suite de signes (2) on rencontre quatre fois des couples de signes opposés voisins. Nous dirons dans ce cas qu'il y a dans la suite ordonnée (1) quatre *changements de signes.* Bien entendu, on peut calculer le *nombre de changements de signes* pour toute suite finie ordonnée de nombres réels non nuls.

Soit maintenant un polynôme à coefficients réels $f(x)$; on peut supposer que $f(x)$ *ne possède pas de zéros multiples*, car, dans le cas contraire, on aurait pu diviser $f(x)$ par le plus grand commun diviseur de $f(x)$ et de sa dérivée $f'(x)$. Une famille finie ordonnée de

polynômes non nuls à coefficients réels

$$f(x) = f_0(x),\ f_1(x),\ f_2(x),\ \ldots,\ f_s(x) \qquad (3)$$

est appelée *famille de Sturm* du polynôme $f(x)$ si les conditions suivantes sont vérifiées :

1. Aucun couple de polynômes voisins de la famille (3) ne possède de zéros communs.
2. Le dernier polynôme $f_s(x)$ n'a pas de zéros réels.
3. Si α est un zéro réel d'un des polynômes $f_k(x)$ de la famille (3) avec $1 \leqslant k \leqslant s-1$, alors $f_{k-1}(\alpha)$ et $f_{k+1}(\alpha)$ sont des nombres réels de signes opposés.
4. Si α est un zéro réel du polynôme $f(x)$, alors le produit $f(x)\,f_1(x)$ change de signe en passant du moins au plus lorsque x croît en passant par le point α.

Le problème d'existence d'une famille de Sturm pour tout polynôme sera considéré ci-dessous; supposant à présent qu'une telle famille existe, montrons comment elle peut être utilisée pour déterminer le nombre de zéros réels de $f(x)$.

Fixons un nombre réel c qui ne soit pas zéro du polynôme $f(x)$; supposons que la famille (3) soit une famille de Sturm de $f(x)$ et formons la suite de nombres réels

$$f(c),\ f_1(c),\ f_2(c),\ \ldots,\ f_s(c),$$

éliminant ceux des membres de cette suite qui sont nuls, désignons par $W(c)$ le nombre de changements de signes dans la suite ordonnée obtenue de cette manière ; $W(c)$ est appelé le *nombre de changements de signes dans la famille de Sturm* (3) *du polynôme* $f(x)$ *pour* $x = c$ [1].

Le théorème suivant est vrai :

Théorème de Sturm. *Soit un polynôme $f(x)$ à zéros tous simples. Supposons que les nombres réels a et b, $a < b$, ne soient pas zéros de $f(x)$; alors on a : $W(a) \geqslant W(b)$ et la différence $W(a) - W(b)$ est égale au nombre des zéros réels du polynôme $f(x)$ compris entre a et b.*

Ainsi, pour déterminer le nombre des zéros réels d'un polynôme $f(x)$, compris entre a et b, il faut seulement calculer la différence entre le nombre de changements de signes dans la famille de Sturm de $f(x)$ pour $x = a$ et pour $x = b$ (rappelons que le polynôme $f(x)$ n'a pas de zéros multiples).

Pour démontrer le théorème considérons le comportement du nombre $W(x)$ lorsque x croît. Tant que x croît sans passer par un zéro des polynômes de la famille de Sturm (3), les signes des polynômes de cette famille ne varient pas et par suite le nombre $W(x)$ conserve sa valeur. Cela étant, il nous reste, en vertu de la condition

[1] Bien entendu, les changements de signes dans la famille de Sturm d'un polynôme $f(x)$ n'ont rien de commun avec les changements de signe du polynôme $f(x)$ lorsque l'indéterminée x passe par les zéros de $f(x)$.

2) de la définition d'une famille de Sturm, à considérer deux cas: le passage de x par un zéro d'un des polynômes intermédiaires $f_k(x)$, $1 \leqslant k \leqslant s-1$, et le passage de x par un zéro du polynôme $f(x)$.

Soit α un zéro du polynôme $f_k(x)$, $1 \leqslant k \leqslant s-1$. Alors, d'après la condition 1), $f_{k-1}(\alpha)$ et $f_{k+1}(\alpha)$ sont non nuls. Donc, on peut trouver un nombre positif ε (probablement très petit) tel que les polynômes $f_{k-1}(x)$ et $f_{k+1}(x)$ n'aient pas de zéros dans l'intervalle $(\alpha-\varepsilon, \alpha+\varepsilon)$ et, par conséquent, conservent leurs signes pour $\alpha-\varepsilon \leqslant x \leqslant \alpha+\varepsilon$, *ces signes étant opposés*, en vertu de la condition 3). Il en résulte que deux suites de nombres

$$f_{k-1}(\alpha-\varepsilon),\ f_k(\alpha-\varepsilon),\ f_{k+1}(\alpha-\varepsilon) \tag{4}$$

et

$$f_{k-1}(\alpha+\varepsilon),\ f_k(\alpha+\varepsilon),\ f_{k+1}(\alpha+\varepsilon) \tag{5}$$

ont chacune un changement de signes indépendamment des signes des nombres $f_k(\alpha-\varepsilon)$ et $f_k(\alpha+\varepsilon)$. Ainsi, supposons, par exemple, que les polynômes $f_{k-1}(x)$ et $f_{k+1}(x)$ soient respectivement négatif et positif dans l'intervalle considéré et que $f_k(\alpha-\varepsilon) > 0$, $f_k(\alpha+\varepsilon) < 0$; alors aux suites (4) et (5) correspondent les suites de signes

$$-,\ +,\ +;\ -,\ -,\ +.$$

Ainsi, lorsque x passe par un zéro d'un des polynômes intermédiaires de la famille de Sturm, les changements de signes peuvent seulement changer de place, mais il est impossible que de nouveaux changements de signes disparaissent ou apparaissent, de sorte que le *nombre $W(x)$ reste invariant pour un tel passage de x.*

D'autre part, soit α un zéro du polynôme $f(x)$. D'après la condition 1) α n'est pas un zéro de $f_1(x)$. Donc, il existe un nombre positif ε tel que l'intervalle $(\alpha-\varepsilon, \alpha+\varepsilon)$ ne contient pas de zéros de $f_1(x)$, de sorte que $f_1(x)$ conserve son signe lorsque $\alpha-\varepsilon \leqslant x \leqslant \alpha+\varepsilon$. Si $f_1(x)$ est positif dans cet intervalle, alors, selon la condition 4), le polynôme $f(x)$ change de signe et devient positif lorsque x, croissant, passe par α, de sorte que l'on a: $f(\alpha-\varepsilon) < 0$, $f(\alpha+\varepsilon) > 0$. Donc, aux suites des nombres

$$f(\alpha-\varepsilon),\ f_1(\alpha-\varepsilon) \quad \text{et} \quad f(\alpha+\varepsilon),\ f_1(\alpha+\varepsilon) \tag{6}$$

correspondent les suites des signes

$$-,\ + \quad \text{et} \quad +,\ +,$$

c'est-à-dire la famille de Sturm *perd un changement de signes*. Si $f_1(x)$ est négatif sur l'intervalle $(\alpha-\varepsilon, \alpha+\varepsilon)$, alors, en vertu de la condition 4), le polynôme $f(x)$ change encore de signe et devient négatif, lorsque x, croissant, passe par α, de sorte que l'on a: $f(\alpha-\varepsilon) > 0$, $f(\alpha+\varepsilon) < 0$: aux suites des nombres (6) correspon-

dent maintenant les suites des signes

$$+,\ -\quad \text{et}\quad -,\ -,$$

c'est-à-dire la famille de Sturm *perd* encore *un changement de signes*.

Ainsi, *le nombre* $W(x)$ *ne varie que lorsque* x, *croissant, passe par un zéro du polynôme* $f(x)$; *en outre, dans ce cas* $W(x)$ *diminue d'une unité.*

Ainsi le théorème de Sturm est démontré. Il suffit, pour l'appliquer au calcul du nombre des zéros réels d'un polynôme $f(x)$, de prendre pour a une borne inférieure des zéros négatifs et pour b une borne supérieure des zéros positifs. Toutefois, il est plus simple de procéder ainsi. D'après le lemme du § 23, il existe un nombre positif N (peut-être très grand) tel que pour $|x| > N$ le signe de tout polynôme d'une famille de Sturm coïncide avec celui de son terme principal. Autrement dit, il existe une valeur positive suffisamment grande de l'indéterminée x telle que la valeur en x de tout polynôme d'une famille de Sturm a le même signe que le *coefficient* du terme principal du polynôme; nous convenons de noter cette valeur de x par le signe ∞ (on n'a pas besoin de la calculer). Il existe, d'autre part, une valeur négative de x, suffisamment grande en valeur absolue, telle que le signe de la valeur de tout polynôme d'une famille de Sturm au point x est le même que celui du coefficient du terme principal si le degré du polynôme est pair et est opposé à celui du coefficient du terme principal si le degré du polynôme est impair; on convient de noter cette valeur de x par $-\infty$. Il est clair que l'intervalle $(-\infty, \infty)$ contient tous les zéros réels de tous les polynômes d'une famille de Sturm et, en particulier, tous les zéros réels du polynôme $f(x)$. Appliquant le théorème de Sturm successivement aux intervalles $(-\infty, \infty)$, $(-\infty, 0)$ et $(0, \infty)$, nous trouverons respectivement le nombre des zéros réels, des zéros négatifs et des zéros positifs du polynôme $f(x)$.

Il reste à montrer que *tout polynôme à coefficients réels* $f(x)$, *n'ayant pas de zéros multiples, possède une famille de Sturm.* Nous donnons ici l'une des méthodes permettant de former une telle famille; cette méthode est le plus souvent utilisée. Posons $f_1(x) = f'(x)$, ce qui garantit que la condition 4) de la définition d'une famille de Sturm est vérifiée. En effet, si α est un zéro réel du polynôme $f(x)$, alors $f'(\alpha) \neq 0$. Soit $f'(\alpha) > 0$, alors $f'(x) > 0$ dans un voisinage du point α, de sorte que $f(x)$ change de signe et devient positif lorsque x, croissant, passe par le point α; alors il en est de même pour le produit $f(x) f_1(x)$. Les mêmes raisonnements sont valables dans le cas où $f'(\alpha) < 0$. Divisons ensuite $f(x)$ par $f_1(x)$; le reste de la division *multiplié par* (-1) est désigné par $f_2(x)$:

$$f(x) = f_1(x)\, q_1(x) - f_2(x).$$

Plus généralement, supposant que les polynômes $f_{k-1}(x)$ et $f_k(x)$ soient déjà trouvés, le polynôme $f_{k+1}(x)$ est le reste de la division de $f_{k-1}(x)$ par $f_k(x)$, multiplié par (-1):

$$f_{k-1}(x) = f_k(x)\,q_k(x) - f_{k+1}(x). \tag{7}$$

La seule différence entre la méthode exposée ci-dessus et l'algorithme d'Euclide, appliqué aux polynômes $f(x)$ et $f'(x)$, consiste en ce que l'on change les signes des restes et que la division s'effectue, ensuite, par le reste dont on a changé le signe. Un tel changement de signes étant sans importance pour le calcul du plus grand commun diviseur, notre processus s'arrêtera lorsque nous aurons trouvé le plus grand commun diviseur $f_s(x)$ des polynômes $f(x)$ et $f'(x)$; or, le polynôme $f(x)$ n'ayant pas de zéros multiples, les polynômes $f(x)$ et $f'(x)$ sont premiers entre eux, de sorte que $f_s(x)$ est, en réalité, un nombre réel non nul.

Il en résulte que la famille de polynômes ainsi formée

$$f(x) = f_0(x),\ f'(x) = f_1(x),\ f_2(x),\ \ldots,\ f_s(x)$$

vérifie la condition 2) de la définition d'une famille de Sturm. Pour démontrer que la condition 1) est aussi satisfaite, supposons qu'un couple de polynômes voisins, soit $f_k(x)$ et $f_{k+1}(x)$, ait un zéro commun α. Alors, selon (7), α est aussi un zéro du polynôme $f_{k-1}(x)$. Passant à l'égalité

$$f_{k-2}(x) = f_{k-1}(x)\,q_{k-1}(x) - f_k(x),$$

il vient que α est un zéro de $f_{k-2}(x)$. Continuant ce processus nous obtiendrons que α est un zéro commun de $f(x)$ et $f'(x)$, ce qui est en contradiction avec notre hypothèse. Enfin, la condition 3) découle directement de l'égalité (7): si $f_k(\alpha) = 0$, alors $f_{k-1}(\alpha) = -f_{k+1}(\alpha)$.

Appliquons la méthode de Sturm au polynôme

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3$$

considéré au paragraphe précédent. Nous n'avons pas besoin de vérifier préalablement que $h(x)$ n'a pas de zéros multiples, car la méthode de construction d'une famille de Sturm ci-dessus sert, en même temps, à vérifier si le polynôme et sa dérivée sont premiers entre eux.

Appliquant la méthode exposée ci-dessus trouvons une famille de Sturm de $h(x)$. Seulement ici, à la différence de l'algorithme d'Euclide, en divisant un polynôme par un autre, nous ne pouvons multiplier et simplifier les polynômes que par des nombres réels *positifs*, les signes des restes jouant un rôle impor-

tant dans la méthode de Sturm. On obtient la famille

$$h\ (x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3,$$
$$h_1(x) = 5x^4 + 8x^3 - 15x^2 + 16x - 7,$$
$$h_2(x) = 66x^3 - 150x^2 + 172x + 61,$$
$$h_3(x) = -464x^2 + 1135x + 723,$$
$$h_4(x) = -32\,599\,457x - 8\,486\,093,$$
$$h_5(x) = -1.$$

Trouvons les signes des polynômes de cette famille pour $x = -\infty$ et $x = \infty$; pour cela, d'après la remarque ci-dessus, il ne faut prendre en considération que les signes des coefficients des termes principaux et les degrés des polynômes en question. Nous obtenons le tableau:

	$h\ (x)$	$h_1(x)$	$h_2(x)$	$h_3(x)$	$h_4(x)$	$h_5(x)$	Nombre de changements de signes
$-\infty$	$-$	$+$	$-$	$-$	$+$	$-$	4
∞	$+$	$+$	$+$		$-$	$-$	1

Ainsi, lorsque x varie de $-\infty$ à ∞, la famille de Sturm perd trois changements de signes; par conséquent, le polynôme $h\ (x)$ possède exactement trois zéros réels. Ainsi le graphe de $h\ (x)$, considéré au paragraphe précédent, donne réellement tous les zéros réels de ce polynôme.

Appliquons la méthode de Sturm à un autre polynôme, plus simple. Soit le polynôme:

$$f\ (x) = x^3 + 3x^2 - 1.$$

Calculons le nombre de ses zéros réels, ainsi que les couples de nombres entiers qui les encadrent; en outre, ne commençons pas par tracer le graphe de ce polynôme.

La famille de polynômes

$$f\ (x) = x^3 + 3x^2 - 1,$$
$$f_1(x) = 3x^2 + 6x,$$
$$f_2(x) = 2x + 1,$$
$$f_3(x) = 1$$

est une famille de Sturm du polynôme $f\ (x)$.

Calculons le nombre de changements de signes dans cette famille respectivement pour $x = -\infty$ et pour $x = \infty$. Il vient:

	$f\ (x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	Nombre de changements de signes
$-\infty$	$-$	$+$	$-$	$+$	3
∞	$+$	$+$	$+$	$+$	0

Ainsi, le polynôme $f(x)$ possède trois zéros réels. Pour préciser la répartition de ces zéros, complétons le tableau précédent :

	$f(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	Nombre de changements de signes
$x=-3$	$-$	$+$	$-$	$+$	3
$x=-2$	$+$	0	$-$	$+$	2
$x=-1$	$+$	$-$	$-$	$+$	2
$x=0$	$-$	0	$+$	$+$	1
$x=1$	$+$	$+$	$+$	$+$	0

Ainsi, la famille de Sturm du polynôme $f(x)$ perd un changement de signes lorsque x varie respectivement entre -3 et -2, entre -1 et 0 et entre 0 et 1. Donc, les zéros α_1, α_2, α_3 de ce polynôme vérifient les inégalités :

$$-3<\alpha_1<-2, \quad -1<\alpha_2<0, \qquad 0<\alpha_3<1.$$

§ 41. Autres théorèmes sur le nombre des zéros réels

Le théorème de Sturm donne la solution complète du problème de calcul du nombre des zéros réels d'un polynôme. Néanmoins, son défaut essentiel consiste en ce que cette méthode nécessite des calculs assez laborieux pour trouver une famille de Sturm ; le lecteur a pu le constater en faisant tous ces calculs pour le premier exemple ci-dessus. Pour cette raison, nous allons démontrer deux théorèmes ne donnant pas le nombre exact des zéros réels, mais limitant *supérieurement* ce nombre. Ces théorèmes permettent quelquefois, après avoir limité *inférieurement* le nombre de zéros réels au moyen du graphe, de trouver le nombre exact des zéros réels sans être obligé de recourir à la méthode de Sturm.

Soit un polynôme $f(x)$ de degré n à coefficients réels ; en outre, on admet qu'il puisse avoir des zéros multiples. Considérons la famille formée par ce polynôme et ses dérivées successives

$$f(x)=f^{(0)}(x), \ f'(x), \ f''(x), \ \ldots, \ f^{(n-1)}(x), \ f^{(n)}(x), \tag{1}$$

dont la dernière est égale au coefficient a_0 du terme principal de $f(x)$ multiplié par $n!$, de sorte que $f^{(n)}(x)$ ne change pas de signe. Soit un nombre réel c tel qu'aucun polynôme de la famille (1) n'ait c

pour zéro ; désignons par $S(c)$ le nombre de changements de signes dans la suite ordonnée des nombres

$$f(c),\ f'(c),\ f''(c),\ \ldots,\ f^{(n-1)}(c),\ f^{(n)}(c).$$

Ainsi, nous avons défini une fonction à valeurs entières $S(x)$ pour toute valeur de x n'annulant pas les polynômes de la famille (1).

Examinons le comportement de $S(x)$ lorsque x croît. Le nombre $S(x)$ ne varie pas tant que x, croissant, ne rencontre pas de zéros des polynômes de la famille (1). Pour cette raison, nous devons considérer deux cas: le passage de x par un zéro du polynôme $f(x)$ et par un zéro d'une des dérivées $f^{(k)}(x)$, $1 \leqslant k \leqslant n-1$.

Soit α un zéro du polynôme $f(x)$ d'ordre de multiplicité l, $l \geqslant 1$, c'est-à-dire

$$f(\alpha)=f'(\alpha)=\ldots=f^{(l-1)}(\alpha)=0,\quad f^{(l)}(\alpha)\neq 0.$$

Soit un nombre positif ε suffisamment petit pour que l'intervalle $(\alpha-\varepsilon, \alpha+\varepsilon)$ ne contienne pas de zéros des polynômes $f(x)$, $f'(x)$, ..., $f^{(l-1)}(x)$, distincts de α, et pour que le polynôme $f^{(l)}(x)$ ne s'annule pas pour $\alpha-\varepsilon \leqslant x \leqslant \alpha+\varepsilon$. Démontrons que dans la suite des nombres

$$f(\alpha-\varepsilon),\ f'(\alpha-\varepsilon),\ \ldots,\ f^{(l-1)}(\alpha-\varepsilon),\ f^{(l)}(\alpha-\varepsilon)$$

tous nombres voisins ont des signes contraires et que les nombres

$$f(\alpha+\varepsilon),\ f'(\alpha+\varepsilon),\ \ldots,\ f^{(l-1)}(\alpha+\varepsilon),\ f^{(l)}(\alpha+\varepsilon)$$

sont tous d'un même signe. Tout polynôme de la famille (1) étant la dérivée première du polynôme qui le précède, il faut démontrer seulement que, indépendamment de l'ordre de multiplicité d'un zéro α de $f(x)$, les polynômes $f(x)$ et $f'(x)$ ont des signes contraires lorsque x est voisin de α et $x<\alpha$, tandis que les signes de $f(x)$ et de $f'(x)$ coïncident lorsque x est voisin de α et $x>\alpha$. Si $f(\alpha-\varepsilon)>0$, alors $f(x)$ décroît sur l'intervalle $(\alpha-\varepsilon, \alpha)$, de sorte que $f'(\alpha-\varepsilon)<0$; si, par contre, $f(\alpha-\varepsilon)<0$, alors $f(x)$ croît et, par conséquent, $f'(\alpha-\varepsilon)>0$. Donc, dans les deux cas les signes de $f(\alpha-\varepsilon)$ et de $f'(\alpha-\varepsilon)$ sont contraires. D'un autre côté, si $f(\alpha+\varepsilon)>0$, alors $f(x)$ croît sur l'intervalle $(\alpha, \alpha+\varepsilon)$ et, par conséquent, $f'(\alpha+\varepsilon)>0$; de façon analogue, l'inégalité $f(\alpha+\varepsilon)<0$ donne $f'(\alpha+\varepsilon)<0$. Ainsi, les signes de $f(x)$ et de $f'(x)$ coïncident après le passage de x par un zéro α de $f(x)$.

Il résulte de la propriété qui vient d'être démontrée que la famille

$$f(x),\ f'(x),\ \ldots,\ f^{(l-1)}(x),\ f^{(l)}(x)$$

perd l changements de signes lorsque x, croissant, passe par un zéro d'ordre de multiplicité l du polynôme $f(x)$.

Maintenant, soit α un zéro des dérivées

$$f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x), \qquad 1 \leqslant k \leqslant n-1,\ l \geqslant 1,$$

et supposons que α ne soit pas un zéro de $f^{(k-1)}(x)$ ni de $f^{(k+l)}(x)$. Selon la propriété démontrée ci-dessus, le passage de x par α entraîne que la famille

$$f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ f^{(k+l)}(x)$$

perd l changements de signes. Il est vrai que cela donne un nouveau changement de signes entre $f^{(k-1)}(x)$ et $f^{(k)}(x)$; toutefois, vu que $l \geqslant 1$, le nombre de changements de signes dans la famille

$$f^{(k-1)}(x),\ f^{(k)}(x),\ f^{(k+1)}(x),\ \ldots,\ f^{(k+l-1)}(x),\ f^{(k+l)}(x)$$

soit ne varie pas, soit diminue, lorsque x, croissant, passe par α. Ce nombre ne peut diminuer que d'un nombre pair, car les polynômes $f^{(k-1)}(x)$ et $f^{(k+l)}(x)$ ne changent pas de signe lorsque x passe par α.

Il s'ensuit des résultats obtenus que *si les nombres a et b, $a < b$, ne sont pas des zéros des polynômes de la famille* (1), *alors le nombre des zéros réels du polynôme $f(x)$, pris avec leurs ordres de multiplicité et compris entre a et b, est égal à $S(a) - S(b)$ ou inférieur à cette différence d'un nombre pair.*

Afin d'affaiblir certaines restrictions sur les nombres a et b, introduisons les notations suivantes. Soit un nombre réel c tel qu'il ne soit pas un zéro du polynôme $f(x)$; le nombre c peut être un zéro de certains polynômes de la famille (1). Désignons par $S_+(c)$ le nombre de changements de signes dans la suite

$$f(c),\ f'(c),\ f''(c),\ \ldots,\ f^{(n-1)}(c),\ f^{(n)}(c), \tag{2}$$

ce nombre devant être calculé de la manière suivante: si

$$f^{(k)}(c) = f^{(k+1)}(c) = \ldots = f^{(k+l-1)}(c) = 0 \tag{3}$$

et

$$f^{(k-1)}(c) \neq 0,\ f^{(k+l)}(c) \neq 0, \tag{4}$$

alors on dit que $f^{(k)}(c)$, $f^{(k+1)}(c)$, ..., $f^{(k+l-1)}(c)$ ont le même signe que $f^{(k+l)}(c)$; il est clair que cela équivaut à éliminer les zéros de la suite (2), en calculant le nombre de changements de signes dans cette suite. D'autre part, désignons par $S_-(c)$ le nombre de changements de signes dans la suite (2), calculé de la manière suivante: si les relations (3) et (4) ont lieu, alors on dit que $f^{(k+i)}(c)$, $0 \leqslant i \leqslant l-1$, a le même signe que $f^{(k+l)}(c)$ quand $l-i$ est pair, et on dit que $f^{(k+i)}(c)$, $0 \leqslant i \leqslant l-1$, a le signe contraire à celui de $f^{(k+l)}(c)$ si $l-i$ est impair.

Maintenant, si l'on veut déterminer le nombre des zéros réels d'un polynôme $f(x)$, compris entre a et b, $a < b$, où a et b ne sont

pas des zéros de $f(x)$ mais peuvent être des zéros d'autres polynômes de la famille (1), on procède alors de la manière suivante. Soit ε un nombre positif si petit que l'intervalle $(a, a+2\varepsilon)$ ne contienne pas de zéros du polynôme $f(x)$, ni des autres polynômes de la famille (1), excepté le zéro a; d'autre part, soit η un nombre positif si petit que l'intervalle $(b-2\eta, b)$ ne contienne pas non plus de zéros de $f(x)$, ni des autres polynômes de (1), excepté, peut-être, le zéro b. Alors, le nombre qui nous intéresse est égal à celui des zéros réels du polynôme $f(x)$ compris entre $a+\varepsilon$ et $b-\eta$, où encore, selon la proposition démontrée ci-dessus, ce nombre est égal à $S(a+\varepsilon)-S(b-\eta)$ (ou il est inférieur à $S(a+\varepsilon)-S(b-\eta)$ d'un nombre pair). Or, il est facile de voir que

$$S(a+\varepsilon)=S_{+}(a), \quad S(b-\eta)=S_{-}(b).$$

Ce qui démontre le théorème suivant:

Théorème de Budan-Fourier. *Soient deux nombres réels a et b, $a<b$, qui ne sont pas des zéros d'un polynôme à coefficients réels $f(x)$. Alors le nombre des zéros réels de $f(x)$, pris avec leurs ordres de multiplicité et compris entre a et b, est égal à la différence $S_{+}(a)-S_{-}(b)$ ou est inférieur à $S_{+}(a)-S_{-}(b)$ d'un nombre pair.*

Désignons par ∞ une valeur positive suffisamment grande de l'indéterminée x telle que les signes des polynômes de la famille (1) au point x soient les mêmes que ceux des coefficients de leurs termes principaux. Ces coefficients étant les nombres a_0, na_0, $n(n-1)a_0$, ..., $n!a_0$, ayant tous le même signe, on a: $S(\infty)=S_{-}(\infty)=0$. D'autre part, vu que

$$f(0)=a_n, \quad f'(0)=a_{n-1}, \quad f''(0)=a_{n-2}2!,$$
$$f'''(0)=a_{n-3}3!, \quad \ldots, \quad f^{(n)}(0)=a_0\cdot n!,$$

où $a_0, a_1, \ldots, a_n$ sont les coefficients du polynôme $f(x)$, on constate que $S_{+}(0)$ coïncide avec le nombre de changements de signes dans la suite ordonnée formée par les coefficients du polynôme $f(x)$; en outre, on doit éliminer les coefficients nuls. Ainsi, appliquant le théorème de Budan-Fourier à l'intervalle $(0, \infty)$, on est conduit au théorème:

Théorème de Descartes. *Le nombre des zéros positifs d'un polynôme $f(x)$ à coefficients réels, chaque zéro étant pris avec son ordre de multiplicité, est égal au nombre de changements de signes dans la suite ordonnée des coefficients de $f(x)$ (les coefficients nuls devant être omis) ou inférieur à ce nombre d'un nombre pair.*

Pour déterminer le nombre de zéros négatifs d'un polynôme $f(x)$, il suffit d'appliquer le théorème de Descartes au polynôme $f(-x)$. En outre, si tous les coefficients de $f(x)$ sont non nuls, alors à tout

changement de signes dans la suite des coefficients de $f(-x)$ correspond une *conservation* de signes dans la suite des coefficients du polynôme $f(x)$ et inversement. Ainsi, *si un polynôme $f(x)$ n'a pas de coefficients nuls, alors le nombre de ses zéros négatifs (pris avec leurs ordres de multiplicité) est égal au nombre de conservations de signes dans la suite des coefficients ou est inférieur à ce nombre d'un nombre pair.*

Donnons *une autre démonstration du théorème de Descartes*, indépendante du théorème de Budan-Fourier. Démontrons d'abord le lemme :

Si $c > 0$, alors le nombre de changements de signes dans la suite ordonnée des coefficients d'un polynôme $f(x)$ est inférieur au nombre de changements de signes dans la suite ordonnée des coefficients du polynôme $(x-c)f(x)$ d'un nombre pair.

En effet, groupant les termes voisins dont les coefficients sont de même signe (le coefficient a_0 du terme principal est supposé positif), mettons le polynôme $f(x)$ sous la forme

$$f(x) = (a_0x^n + \ldots + b_1x^{k_1+1}) - (a_1x^{k_1} + \ldots$$
$$\ldots + b_2x^{k_2+1}) + \ldots + (-1)^s(a_sx^{k_s} + \ldots + b_{s+1}x^t). \qquad (5)$$

Ici $a_0 > 0$, $a_1 > 0$, ..., $a_s > 0$ et b_1, b_2, ..., b_s sont non négatifs ; mais nous supposons que b_{s+1} est strictement positif, c'est-à-dire que x^t, $t \geqslant 0$, est la puissance de l'indéterminée x d'exposant le plus petit qui intervient dans l'expression du polynôme $f(x)$ avec un coefficient non nul. Il est possible que la parenthèse

$$(a_0x^n + \ldots + b_1x^{k_1+1})$$

ne contienne qu'un terme : notamment, cela a lieu si $k_1 + 1 = n$. Les remarques analogues sont vraies pour les autres parenthèses dans la formule (5).

Maintenant, écrivons le polynôme $(x-c)f(x)$, en mettant en évidence seulement les termes en x élevé aux puissances $n+1$, k_1+1, ..., k_s+1 et t. Il vient :

$$(x-c)f(x) = (a_0x^{n+1} + \ldots) - (a'_1x^{k_1+1} + \ldots) + \ldots$$
$$\ldots + (-1)^s(a'_sx^{k_s+1} + \ldots - cb_{s+1}x^t), \qquad (6)$$

où $a'_i = a_i + cb_i$, $i = 1, 2, \ldots, s$, de sorte que a'_i sont strictement positifs, car $c > 0$. Ainsi, dans la suite des coefficients du polynôme $f(x)$ entre les termes a_0x^n et $-a_1x^{k_1}$ (ainsi qu'entre les termes $-a_1x^{k_1}$ et $a_2x^{k_2}$, etc.) il y a exactement un changement de signes, tandis que dans la suite des coefficients du polynôme $(x-c)f(x)$ entre les termes correspondants a_0x^{n+1} et $-a'_1x^{k_1+1}$ (respectivement entre les termes $-a'_1x^{k_1+1}$ et $a'_2x^{k_2+1}$, etc.) il y a soit un changement de

signes, soit plus d'un changement de signes, mais alors ce dernier nombre doit être impair. Les endroits où se trouvent ces changements de signes ne nous intéressent point; par exemple, il peut arriver que le coefficient de x^{k_1+2} dans (6) soit négatif, tout comme le coefficient $-a_1'$, de sorte qu'il n'y a pas de changements de signes entre ces deux coefficients voisins; cela signifie que dans la première parenthèse les changements de signes précèdent les termes en question. Remarquons maintenant que la dernière parenthèse dans (5) n'a pas de changements de signes, tandis que celle dans (6) en a un nombre impair: pour cela, il suffit de prendre en considération que les derniers coefficients non nuls des polynômes $f(x)$ et $(x-c)\ f(x)$, c'est-à-dire les nombres $(-1)^s b_{s+1}$ et $(-1)^{s+1} b_{s+1}\, c$, ont des signes contraires. Ainsi, lorsqu'on passe du polynôme $f(x)$ au polynôme $(x-c)\ f(c)$, le nombre total de changements de signes dans la suite des coefficients augmente d'un nombre impair (la somme d'un certain nombre de termes pairs et d'un terme impair donne, bien entendu, un nombre impair!). Le lemme est démontré.

Pour démontrer maintenant le théorème de Descartes, notons par $\alpha_1, \alpha_2, \ldots, \alpha_k$ les zéros positifs du polynôme $f(x)$. Ainsi, on a

$$f(x) = (x-\alpha_1)(x-\alpha_2)\ \ldots\ (x-\alpha_k)\ \varphi(x),$$

où $\varphi(x)$ est un polynôme à coefficients réels sans zéros réels positifs. Il en résulte que le premier et le dernier coefficient non nul de $\varphi(x)$ sont de même signe, c'est-à-dire dans la suite des coefficients du polynôme $\varphi(x)$ il y a un nombre pair de changements de signes. Appliquant le lemme démontré ci-dessus successivement aux polynômes

$$\varphi(x),\ (x-\alpha_1)\varphi(x),\ (x-\alpha_1)(x-\alpha_2)\varphi(x),\ \ldots,\ f(x),$$

nous obtenons que le nombre de changements de signes dans la suite ordonnée des coefficients augmente chaque fois d'un nombre impair, de sorte que le nombre de changements de signes dans la suite des coefficients du polynôme $f(x)$ est supérieur à k d'un nombre pair.

Appliquons le théorème de Descartes et le théorème de Budan-Fourier au polynôme

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3,$$

considéré ci-dessus.

Le nombre de changements de signes dans la suite des coefficients est égal à trois, de sorte que, d'après le théorème de Descartes, $h(x)$ peut avoir soit un zéro positif, soit trois. D'autre part, $h(x)$ n'ayant pas de coefficients nuls et vu que dans la suite des coefficients de $h(x)$ il y a exactement deux conservations de signes, le polynôme $h(x)$ peut avoir deux zéros négatifs ou bien n'a pas du tout de zéros négatifs. Comparant ces résultats avec ceux obtenus précédemment, au moyen du graphe, nous constatons que $h(x)$ possède exactement deux zéros négatifs.

Pour déterminer le nombre exact des zéros positifs appliquons le théorème de Budan-Fourier dans l'intervalle $(1, \infty)$, car on a déjà montré au § 39 que

1 est une borne inférieure des zéros positifs du polynôme $h(x)$. Les dérivées successives ont été également calculées au § 39. Trouvons leurs signes pour $x = 1$ et $x = \infty$:

	$h(x)$	$h'(x)$	$h''(x)$	$h'''(x)$	$h^{IV}(x)$	$h^{V}(x)$	Nombre de changements de signes
$x=1$	$-$	$+$	$+$	$+$	$+$	$+$	1
$x=\infty$	$+$	$+$	$+$	$+$	$+$	$+$	0

Il en résulte que la famille des dérivées perd un changement de signes lorsque x varie entre 1 et ∞, et, par conséquent, $h(x)$ a exactement un zéro positif.

A propos de cet exemple remarquons que *pour déterminer le nombre des zéros réels d'un polynôme il faut, dans le cas général, commencer par tracer le graphe de ce polynôme et utiliser ensuite les théorèmes de Descartes et de Budan-Fourier ; ce n'est que dans les cas extrêmes qu'il faut former la famille de Sturm du polynôme en question.*

Le théorème de Descartes peut être précisé dans le cas particulier où l'on sait dès le début que tous les zéros du polynôme sont réels, comme, par exemple, dans le cas du polynôme caractéristique d'une matrice symétrique. Notamment :

Soit un polynôme $f(x)$ dont les zéros sont réels et le terme indépendant de x est non nul ; alors le nombre k_1 des zéros positifs de ce polynôme est é g a l au nombre s_1 des changements de signes dans la suite des coefficients tandis que le nombre k_2 des zéros négatifs est égal au nombre s_2 des changements de signes dans la suite des coefficients du polynôme $f(-x)$.

En effet, d'après nos hypothèses on a

$$k_1 + k_2 = n, \tag{7}$$

n étant le degré du polynôme $f(x)$, et, en vertu du théorème de Descartes, les inégalités

$$k_1 \leqslant s_1, \quad k_2 \leqslant s_2 \tag{8}$$

ont lieu. Démontrons que

$$s_1 + s_2 \leqslant n. \tag{9}$$

Utilisons la récurrence sur n pour la démonstration de (9) ; pour $n = 1$, vu que $a_0 \neq 0$ et $a_1 \neq 0$, il n'y a qu'un des polynômes

$$f(x) = a_0x + a_1, \quad f(-x) = -a_0x + a_1,$$

dont la suite des coefficients possède un changement de signes, c'est-à-dire dans ce cas $s_1 + s_2 = 1$. Supposons que la formule (9)

soit démontrée pour tout polynôme de degré strictement inférieur à n. Soit

$$f(x) = a_0 x^n + a_{n-l} x^l + \dots + a_n,$$

où $l \leqslant n-1$, $a_{n-l} \neq 0$, posons

$$g(x) = a_{n-l} x^l + \dots + a_n.$$

Alors

$$f(x) = a_0 x^n + g(x), \quad f(-x) = (-1)^n a_0 x^n + g(-x).$$

Soient s_1' et s_2' les nombres de changements de signes dans les suites des coefficients respectivement du polynôme $g(x)$ et du polynôme $g(-x)$; alors, d'après l'hypothèse de récurrence (il est clair que $l \geqslant 1$), on a

$$s_1' + s_2' \leqslant l.$$

Si $l = n - 1$, alors le premier changement de signes, c'est-à-dire celui provenant des coefficients a_0 et $a_1 = a_{n-l}$ de $f(x)$, peut avoir lieu seulement pour l'un des polynômes $f(x)$ et $f(-x)$, de sorte que l'on a

$$s_1 + s_2 = s_1' + s_2' + 1 \leqslant l + 1 = n.$$

Si $l \leqslant n - 2$, les changements de signes provenant des coefficients a_0 et a_{n-l} peuvent avoir lieu pour les deux polynômes $f(x)$ et $f(-x)$; néanmoins, dans ce cas on a également

$$s_1 + s_2 \leqslant s_1' + s_2' + 2 \leqslant l + 2 \leqslant (n-2) + 2 = n.$$

Comparant (7), (8) et (9), il vient:

$$k_1 = s_1, \qquad k_2 = s_2,$$

ce qu'il fallait démontrer.

§ 42. Calcul approché des zéros

Les méthodes exposées aux paragraphes précédents permettent de séparer les zéros réels d'un polynôme $f(x)$ à coefficients réels, c'est-à-dire de mettre en évidence pour tout zéro un intervalle qui ne contient que ce zéro du polynôme. Si l'intervalle est assez petit, on peut prendre pour valeur approchée du zéro tout nombre appartenant à cet intervalle. Ainsi, ayant établi par la méthode de Sturm (ou par une méthode plus économe) que des nombres *rationnels* a et b encadrent exactement un zéro du polynôme $f(x)$, il reste le problème de savoir de combien on doit resserrer l'intervalle (a, b) pour que les extrémités a' et b' du nouvel intervalle soient des nombres

rationnels dont un nombre donné des premières décimales coïncide; ainsi, le zéro cherché sera calculé avec une précision donnée.

Il existe plusieurs méthodes permettant de calculer assez rapidement et avec une précision donnée les valeurs approchées des zéros d'un polynôme. Nous n'en indiquerons que deux; ces méthodes sont assez simples du point de vue théorique et, en même temps, ont un caractère général; en outre, alternant ces deux méthodes on obtient assez rapidement le résultat en vue. Il faut remarquer que les méthodes qui seront exposées sont valables non seulement pour les polynômes, mais aussi pour des classes plus générales de fonctions continues.

Dans tout ce qui suit α est supposé être un zéro *simple* d'un polynôme $f(x)$, car on peut toujours se débarrasser des zéros multiples; en outre, on suppose que le zéro α soit déjà séparé: $a < \alpha < b$; il en résulte, en particulier, que $f(a)$ et $f(b)$ sont de signes opposés.

Méthode d'interpolation linéaire. On peut prendre comme valeur approchée du zéro α, par exemple, la moyenne arithmétique $\frac{a+b}{2}$ des nombres a et b encadrant α, c'est-à-dire le centre de l'intervalle dont les extrémités sont respectivement a et b. Toutefois, il est plus naturel de supposer que le zéro est situé plus près de l'extrémité où la valeur absolue du polynôme est plus petite. La méthode d'interpolation linéaire consiste en ce qu'on choisit pour valeur approchée du zéro α un nombre c tel qu'il divise l'intervalle (a, b) en deux sous-intervalles dont les longueurs sont proportionnelles aux valeurs absolues des nombres $f(a)$ et $f(b)$, c'est-à-dire

$$\frac{c-a}{b-c} = -\frac{f(a)}{f(b)};$$

le signe moins dans le second membre est dû à ce fait que $f(a)$ et $f(b)$ sont de signes opposés. On en déduit

$$c = \frac{bf(a)-af(b)}{f(a)-f(b)}. \tag{1}$$

Du point de vue géométrique, la méthode d'interpolation linéaire signifie que l'on remplace dans l'intervalle (a, b) la courbe $y = f(x)$ par la corde joignant les points $(a, f(a))$ et $(b, f(b))$ et que l'on prend pour valeur approchée du zéro α l'abscisse du point d'intersection de cette corde avec l'axe des abscisses (fig. 10).

Méthode de Newton. Le zéro α du polynôme $f(x)$ étant simple, on a $f'(\alpha) \neq 0$. Supposons, en outre, que $f''(\alpha) \neq 0$, car, dans le cas contraire, nous aurions le même problème pour le polynôme $f''(x)$ qui est de degré inférieur à celui de $f(x)$. Supposons encore que l'intervalle (a, b) ne contienne pas de zéros de $f(x)$ distincts de α,

mais aussi aucun zéro des polynômes $f'(x)$ et $f''(x)$ [1]. Ainsi, il vient du cours d'analyse que la courbe $y = f(x)$ dans l'intervalle (a, b) croît ou décroît de façon monotone; en outre, cette courbe est soit convexe, soit concave dans tout l'intervalle. Donc, la courbe $y = f(x)$ peut se comporter dans l'intervalle (a, b) de quatre manières différentes représentées sur les figures 11-14.

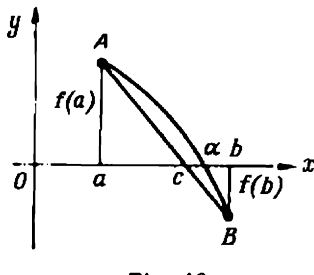


Fig. 10

Désignons par a_0 l'extrémité de l'intervalle (a, b) où *les signes de* $f(x)$ *et de* $f''(x)$ *coïncident*. Les nombres $f(a)$ et $f(b)$ ayant des signes contraires et $f''(x)$ conservant son signe pour $a < x < b$, un tel nombre a_0 peut être trouvé. Sur les figures 11 et 14, on a: $a_0 = a$, sur les deux autres figures $a_0 = b$. Menons la tangente à la courbe $y = f(x)$ au point d'abscisse a_0, c'est-à-dire au point $(a_0, f(a_0))$; soit d l'abscisse du point d'intersection de la tangente

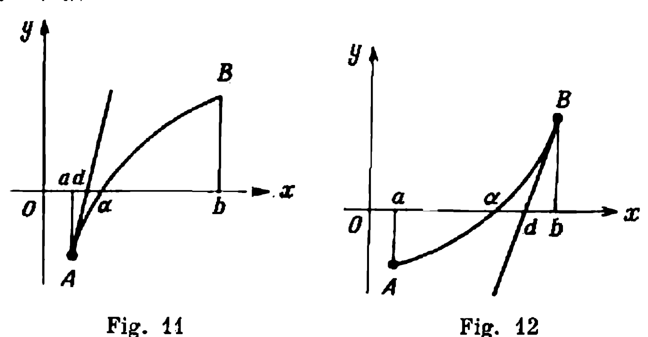


Fig. 11 Fig. 12

et de l'axe des abscisses. Les figures 11-14 montrent que le nombre d peut être pris pour valeur approchée du zéro α. La méthode de Newton est, donc, équivalente au procédé suivant: on remplace dans l'intervalle (a, b) la courbe $y = f(x)$ par une tangente à cette courbe passant par l'un des points $(a, f(a))$ et $(b, f(b))$. La condition imposée sur le choix du point a_0 est essentielle; en effet, la figure 15 montre que si cette condition n'est pas satisfaite, alors il peut arriver que le point d'intersection de la tangente et de l'axe des abscisses n'approche pas le zéro cherché.

---

[1] Le resserrement de l'intervalle qui nous conduit inévitablement à la situation où ces conditions sont satisfaites peut être réalisé sans aucune peine, car les méthodes exposées ci-dessus permettent de déterminer le nombre de zéros des polynômes $f'(x)$ et $f''(x)$ dans tout intervalle.

Etablissons la formule qui donne le nombre d. On sait que l'équation d'une tangente à la courbe $y = f(x)$ en un point $(a_0, f(a_0))$ peut être mise sous la forme

$$y - f(a_0) = f'(a_0)(x - a_0).$$

Remplaçant dans cette équation le point (x, y) par le point $(d, 0)$, point d'intersection de la tangente et de l'axe des abscisses, il vient :

$$-f(a_0) = f'(a_0)(d - a_0),$$

d'où l'on a

$$d = a_0 - \frac{f(a_0)}{f'(a_0)}. \tag{2}$$

Traçant le segment joignant les points A et B sur les figures 11-14, le lecteur peut constater que *la méthode d'interpolation linéaire*

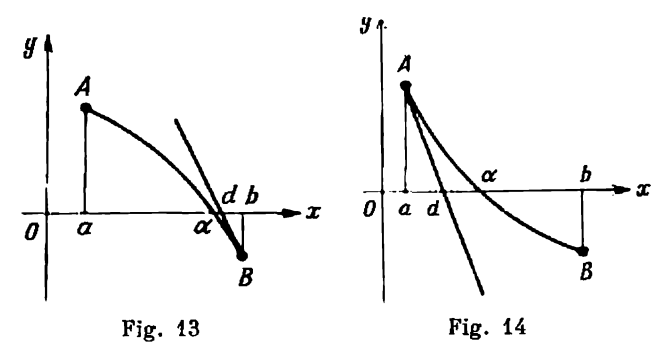


Fig. 13 Fig. 14

et celle de Newton donnent, dans tous les cas, deux valeurs approchées du zéro α qui encadrent ce dernier. Ainsi, il est utile d'*alterner*

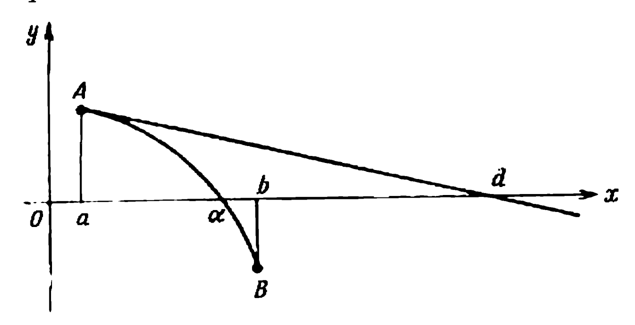


Fig. 15

ces deux méthodes, à condition, bien entendu, que le segment (a, b) satisfasse aux conditions de la méthode de Newton. De cette manière

nous resserrerons l'intervalle contenant le zéro α ; si les extrémités c et d de cet intervalle ne donnent pas encore la précision désirée, il faut alors appliquer encore une fois les deux méthodes indiquées ci-dessus (fig. 16) à l'intervalle (c, d), etc. ; en outre, on peut démontrer que ce processus itératif permet de calculer la valeur approchée du zéro α avec une précision arbitrairement grande.

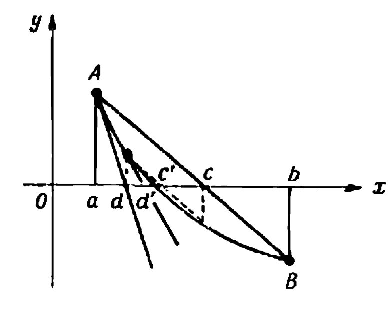


Fig. 16

Appliquons ces deux méthodes au polynôme

$$h(x) = x^5 + 2x^4 - 5x^3 + 8x^2 - 7x - 3$$

considéré dans les paragraphes précédents.

On sait que ce polynôme a un zéro simple α_1 compris entre les nombres 1 et 2 : $1 < \alpha_1 < 2$. Il faut dire tout de suite que cet intervalle est trop grand pour que la méthode d'interpolation linéaire et celle de Newton, appliquées chacune une fois, donnent un bon résultat. Appliquons-les quand même afin que nous ayons au moins un exemple qui ne nécessite pas de calculs laborieux.

On a déjà vu au paragraphe précédent que les dérivées $h'(x)$, $h''(x)$, ..., $h^{V}(x)$ ont des valeurs positives pour $x = 1$. Il en résulte, d'après les résultats du § 39, que la valeur $x = 1$ est une borne supérieure des zéros positifs des polynômes $h'(x)$ et $h''(x)$. Donc, le segment (1, 2) ne contient pas de zéros de ces dérivées et, par conséquent, la méthode de Newton peut être appliquée. En outre, $h''(x)$ est positif pour tout x appartenant à ce segment et, vu que

$$h(1) = -4, \quad h(2) = 39,$$

on doit poser : $a_0 = 2$. Etant donné que $h'(2) = 109$, la formule (2) donne :

$$d = 2 - \frac{39}{109} = \frac{179}{109} = 1{,}64 \ldots$$

D'autre part, la formule (1) donne :

$$c = \frac{2 \cdot (-4) - 1 \cdot 39}{-4 - 39} = \frac{47}{43} = 1{,}09 \ldots$$

et, par conséquent, le zéro α_1 est compris entre les limites

$$1{,}09 < \alpha_1 < 1{,}65.$$

Nous avons obtenu un resserrement de l'intervalle, contenant le zéro, qui ne peut pas être considéré comme satisfaisant. Bien entendu, on pourrait appliquer de nouveau nos méthodes à l'intervalle obtenu. Toutefois, il est utile de trouver dès le début deux nombres encadrant le zéro α_1 et tels que leur différence soit, par exemple, inférieure à 0,1 ou même à 0,01, et appliquer ensuite nos méthodes. Bien sûr, cela nécessitera des calculs laborieux, mais ils sont inévitables lorsqu'on aborde des problèmes concrets où l'on veut calculer les zéros avec une bonne précision.

Revenons à notre polynôme $h(x)$ et à son zéro α_1. Le calcul des valeurs des polynômes qui suit est donné par le procédé de Hörner. Vu que

$$h(1{,}3) = -0{,}13987, \quad h(1{,}31) = 0{,}0662923851,$$

on a

$$1{,}3 < \alpha_1 < 1{,}31,$$

c'est-à-dire nous avons calculé le zéro α_1 avec une erreur inférieure à 0,01. Appliquons maintenant à ce nouveau segment la méthode d'interpolation linéaire :

$$c = \frac{1{,}31\cdot(-0{,}13987)-1{,}3\cdot 0{,}0662923851}{-0{,}13987-0{,}0662923851} = \frac{0{,}26940980063}{0{,}2061623851} = 1{,}30678\ldots$$

Appliquons à ce même intervalle la méthode de Newton, en posant $a_0 = 1{,}31$. Vu que

$$h'(1{,}31) = 20{,}92822405,$$

on a

$$d = 1{,}31 - \frac{0{,}0662923851}{20{,}92822405} = \frac{27{,}3496811204}{20{,}92822405} = 1{,}30683\ldots$$

Ainsi,

$$1{,}30678 < \alpha_1 < 1{,}30684,$$

et, posant $\alpha_1 = 1{,}30681$, nous faisons une erreur inférieure à 0,00003.

Jusqu'ici nous n'avons pas montré que les méthodes exposées ci-dessus permettent de calculer un zéro avec une erreur arbitrairement petite, c'est-à-dire nous n'avons pas encore démontré la convergence de ces méthodes. Démontrons-le au moins pour la méthode de Newton.

Soit α un zéro simple d'un polynôme $f(x)$ dans un intervalle (a, b) ; en outre, supposons que l'intervalle (a, b) vérifie les conditions de la méthode de Newton. En particulier, il en résulte l'existence de deux nombres positifs A et B tels que l'on ait pour tout x sur le segment (a, b) :

$$|f'(x)| > A, \qquad |f''(x)| < B. \tag{3}$$

Introduisons la notation

$$C = \frac{B}{2A}$$

et supposons que

$$C(b-a) < 1. \tag{4}$$

Pour satisfaire cette dernière inégalité il faudra, peut-être, resserrer le segment (a, b); or, cela ne peut pas altérer les inégalités (3). Soit a_0 l'extrémité du segment (a, b) par laquelle il faut commencer à appliquer la méthode de Newton. D'après la formule (2), nous obtenons une suite de valeurs approchées du zéro α, soit $a_1, a_2, \ldots, a_k, \ldots$; tous les a_k appartiennent au segment (a, b) et sont liés entre eux par les égalités

$$a_k = a_{k-1} - \frac{f(a_{k-1})}{f'(a_{k-1})}, \qquad k = 1, 2, \ldots \tag{5}$$

Soit

$$\alpha = a_k + h_k, \qquad k = 0, 1, 2, \ldots \tag{6}$$

Alors

$$0 = f(\alpha) = f(a_k) + h_k f'(a_k) + \frac{h_k^2}{2} f''(a_k + \theta h_k),$$

où $0 < \theta < 1$. Vu que $f'(a_k) \neq 0$ en vertu de la condition imposée au segment (a, b), et compte tenu de (5) et de (6), il vient :

$$-\frac{h_k^2}{2} \frac{f''(a_k + \theta h_k)}{f'(a_k)} = h_k + \frac{f(a_k)}{f'(a_k)} = \alpha - \left(a_k - \frac{f(a_k)}{f'(a_k)}\right) = \alpha - a_{k+1} = h_{k+1}.$$

On en déduit

$$|h_{k+1}| = h_k^2 \left| \frac{f''(a_k + \theta h_k)}{2f'(a_k)} \right| < h_k^2 \frac{B}{2A} = Ch_k^2, \quad k = 0, 1, 2, \ldots$$

Ainsi,

$$|h_{k+1}| < Ch_k^2 < C^3 h_{k-1}^4 < C^7 h_{k-2}^8 < \ldots < C^{2^{k+1}-1} h_0^{2^{k+1}}$$

ou encore, vu que $|h_0| = |\alpha - a_0| < b - a$, on a

$$|h_{k+1}| < C^{-1} [C(b-a)]^{2^{k+1}}, \qquad k = 0, 1, 2, \ldots \tag{7}$$

Il en résulte, vu la condition (4), que *la différence h_k entre le zéro α et sa valeur approchée a_k, obtenue par l'application successive de la méthode de Newton, tend vers zéro lorsque k tend vers l'infini*, ce qu'il fallait démontrer.

Notons que la formule (7) donne une *estimation de l'erreur* commise pour la $(k + 1)^{\text{ème}}$ itération de la méthode de Newton, ce qui est essentiel si l'on applique uniquement cette méthode sans l'alterner avec celle d'interpolation linéaire.

Le lecteur trouvera dans les cours de calcul approché des procédés de calcul plus rationnels, qui facilitent l'application des méthodes ci-dessus, ainsi que d'autres méthodes dont *celle de Lobatchevski* (quelquefois, on l'appelle par erreur méthode de Graeffe). Cette dernière méthode permet de calculer les valeurs approchées de tous les zéros simultanément, y compris les zéros complexes ; en outre, elle n'exige pas, pour son application, la séparation des zéros ; toutefois, cette méthode nécessite des calculs très laborieux. Elle est basée sur la théorie des polynômes symétriques qui sera exposée dans le chapitre XI.

§ 43. Anneaux et champs numériques

Dans la plupart des chapitres précédents de notre cours, nous nous sommes trouvés dans la situation où, pour exposer telle ou telle théorie, nous nous placions soit dans le cas des nombres complexes, soit seulement dans le cas des nombres réels; mais ensuite nous étions obligés de noter que les résultats obtenus restaient vrais si l'on se bornait aux nombres réels et, respectivement, qu'ils pouvaient être généralisés au cas des nombres complexes. En outre, on aurait pu remarquer que dans ces cas, les théories exposées étaient, en règle générale, valables même si l'on ne considérait que les nombres rationnels. Il est temps de montrer au lecteur les raisons véritables de ce parallélisme afin que nous puissions exposer ultérieurement le matériel dans toute sa généralité, c'est-à-dire en utilisant le langage algébrique adapté à ce propos. A ce dessein, nous introduisons d'abord la notion de *champs* ainsi qu'une notion encore plus générale, mais qui joue un rôle auxiliaire dans notre cours, à savoir celle d'*anneau*.

Il est clair que l'ensemble des nombres complexes, ceux des nombres réels et des nombres rationnels, ainsi que l'ensemble des nombres entiers, *jouissent d'une même propriété*: *dans chacun de ces ensembles on peut non seulement additionner et multiplier les éléments, mais aussi retrancher un élément d'un autre, la différence étant un élément de l'ensemble considéré.* Cette propriété fait distinguer ces ensembles, par exemple, de l'ensemble des nombres entiers positifs ou de celui des nombres réels positifs.

Tout ensemble numérique, complexe ou réel, qui contient la somme, la différence et le produit de tout couple d'éléments, est appelé *anneau numérique*. Ainsi, les ensembles des nombres entiers, rationnels, réels et complexes forment chacun un anneau numérique. D'autre part, aucun ensemble formé par des nombres positifs ne peut être un anneau, car pour tout couple de nombres distincts a et b de cet ensemble, soit la différence $a - b$, soit la différence $b - a$ est négative. Aucun sous-ensemble de l'ensemble des nombres négatifs ne saurait non plus être un anneau, ne serait-ce que parce que le produit de deux nombres négatifs est un nombre positif.

Les quatre exemples cités sont bien loin d'épuiser tous les exemples d'anneaux numériques. Nous allons donner encore quelques exemples; en outre, on laisse au lecteur le soin de vérifier que les ensembles qu'on va considérer forment réellement des anneaux numériques.

Les nombres pairs forment un anneau; plus généralement, pour tout entier positif n, l'ensemble des nombres entiers, positifs et négatifs, divisibles par n, forme un anneau. Les nombres impairs ne peuvent pas constituer un anneau, car la somme de deux nombres impairs est un nombre pair.

Les nombres rationnels, dont les dénominateurs sont des puissances de 2, forment un anneau (on suppose que la fraction qui représente le nombre rationnel ne peut pas être simplifiée); en particulier, les nombres entiers appartiennent à cet ensemble, car on peut dire que les fractions qui les représentent ont pour dénominateur l'unité, c'est-à-dire 2 à la puissance zéro. On pourrait remplacer, dans cet exemple, le nombre 2 par un nombre premier p. Plus généralement, fixant un ensemble des nombres premiers (fini ou infini) et considérant les nombres rationnels dont les dénominateurs ne sont divisibles que par les nombres premiers appartenant à l'ensemble fixé, nous obtenons un anneau. D'autre part, l'ensemble des nombres rationnels, dont les dénominateurs ne sont pas divisibles par le carré de tout nombre premier, n'est pas un anneau, car la propriété indiquée de ces nombres n'est pas conservée après leur multiplication.

Passons aux exemples d'anneaux numériques dont les éléments ne sont pas tous des nombres rationnels. L'ensemble des nombres de la forme

$$a+b\sqrt{2}, \tag{1}$$

où a et b sont rationnels, est un anneau; cet anneau contient, comme cas particulier, l'anneau des nombres rationnels ($b = 0$) et le nombre $\sqrt{2}$ ($a = 0$, $b = 1$). En nous limitant aux coefficients a et b entiers dans la formule (1), nous obtenons également un anneau. Bien entendu, dans ces exemples on peut remplacer $\sqrt{2}$ par $\sqrt{3}$ ou bien par $\sqrt{5}$, etc.

L'ensemble des nombres de la forme

$$a+b\sqrt[3]{2} \tag{2}$$

à coefficients rationnels (ou entiers) a et b n'est pas un anneau, car le produit du nombre $\sqrt[3]{2}$ par lui-même ne peut pas être représenté sous la forme (2), comme il est facile de vérifier [1].

---

[1] En effet, soit

$$\sqrt[3]{4}=a+b\sqrt[3]{2}, \tag{2'}$$

Toutefois, l'ensemble des nombres

$$a+b\sqrt[3]{2}+c\sqrt[3]{4}, \tag{3}$$

avec a, b, c rationnels quelconques, est déjà un anneau; la même chose est vraie si dans (3) a, b et c sont des entiers quelconques.

Considérons maintenant les nombres réels qui peuvent être obtenus en appliquant plusieurs fois les opérations d'addition, de multiplication et de soustraction au nombre π (bien connu du lecteur) et aux nombres rationnels quelconques. Les nombres qui s'en obtiennent peuvent être mis sous la forme

$$a_0+a_1\pi+a_2\pi^2+\ldots+a_n\pi^n, \tag{4}$$

avec a_0, a_1, . . ., a_n rationnels et n entier, $n\geqslant 0$. Notons qu'il n'existe pas de nombres qui aient deux formes (4) distinctes, sinon, retranchant l'une de ces représentations de l'autre, nous obtiendrions pour le nombre π une équation polynomiale à coefficients rationnels; or, utilisant les méthodes d'analyse on démontre que le nombre π ne saurait pas satisfaire à une telle équation, c'est-à-dire que le nombre π est transcendant. Toutefois, on peut démontrer, sans utiliser ce résultat, c'est-à-dire ne supposant pas l'unicité de la représentation (4), que les nombres (4) forment un anneau.

Les nombres que l'on obtient des nombres rationnels et du nombre π au moyen des opérations d'addition, de multiplication, de soustraction et de division, appliquées un certain nombre de fois, forment également un anneau. Pour le démontrer il n'est pas besoin de chercher une bonne écriture appropriée de ces nombres (bien qu'on puisse la trouver), il suffit de remarquer que si les nombres α et β sont obtenus du nombre π et des nombres rationnels au moyen des opérations citées ci-dessus, il en est de même pour les nombres $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ et $\frac{\alpha}{\beta}$ (avec $\beta\neq 0$).

---

avec a et b rationnels. Multipliant les deux membres par $\sqrt[3]{2}$, il vient:

$$2=a\sqrt[3]{2}+b\sqrt[3]{4}.$$

Remplaçant $\sqrt[3]{4}$ par son expression (2′) nous obtenons après quelques simplifications évidentes l'égalité

$$(a+b^2)\sqrt[3]{2}=2-ab. \tag{2″}$$

Si $a+b^2\neq 0$, alors

$$\sqrt[3]{2}=\frac{2-ab}{a+b^2};$$

or, cela est impossible, le second membre étant un nombre rationnel. Si, par contre, $a+b^2=0$, alors, selon (2″), on a également: $2-ab=0$. Ces deux égalités donnent: $b^3=-2$, ce qui est impossible, car b est rationnel.

Enfin, l'ensemble des nombres complexes $a + bi$ avec a et b *rationnels* est un anneau; le même résultat est vrai si nous prenons a et b *entiers*.

Les exemples considérés ne sauraient pas donner une idée de la grande diversité des anneaux numériques. Néanmoins, nous n'allons pas allonger la liste des exemples et passons à l'examen d'un type spécial mais très important d'anneaux numériques. On sait que la division par un nombre non nul peut être réalisée dans les ensembles des nombres rationnels, réels et complexes, tandis que dans l'ensemble des nombres entiers la division nous conduit à des éléments n'appartenant pas à cet ensemble. Jusqu'ici nous n'avions pas fait attention à cette distinction; en réalité, elle est essentielle et nous conduit à la définition suivante.

Un anneau numérique est dit *champ numérique* s'il contient le quotient de tout couple de nombres qui lui appartiennent (bien entendu, le diviseur est supposé non nul). Donc, on peut parler des champs des nombres rationnels, réels et complexes, tandis que l'anneau des nombres entiers n'est pas un champ.

Certains anneaux considérés dans les exemples ci-dessus sont, en réalité, des champs. D'abord, notons qu'il n'existe pas de champs numériques, sous-ensembles de l'ensemble des nombres rationnels (l'ensemble formé par un élément nul n'est pas considéré comme un champ).

Une proposition encore plus générale est vraie:

Tout champ numérique contient le champ des nombres rationnels.

En effet, soit un champ numérique que l'on note par P. Si a est un nombre non nul de P, alors P contient également le quotient de la division de a par lui-même, c'est-à-dire le nombre un. Additionnant le nombre un n fois, nous obtenons que les nombres entiers positifs appartiennent à P. D'autre part, le champ P contient le zéro, de sorte qu'il contient la différence du zéro et de tout nombre entier positif, c'est-à-dire les nombres entiers négatifs. Enfin, les quotients de deux nombres entiers quelconques, c'est-à-dire les nombres rationnels, sont également des éléments du champ P.

Le champ des nombres complexes contient une multitude de sous-champs différents dont celui des nombres rationnels est le plus petit. Ainsi, l'anneau considéré ci-dessus formé par les nombres de la forme

$$a+b\sqrt{2} \qquad (5)$$

avec a et b *rationnels quelconques* (et non seulement entiers) est un champ. En effet, considérons le quotient de deux nombres de la forme (5), soient $a + b\sqrt{2}$ et $c + d\sqrt{2}$; en outre, $c + d\sqrt{2}$ est supposé différent de zéro. Par conséquent, le nombre $c - d\sqrt{2}$ est

également non nul, de sorte que

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{(c+d\sqrt{2})(c-d\sqrt{2})}=\frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\sqrt{2}.$$

Nous avons encore obtenu un nombre du type (5) avec des coefficients rationnels. Bien entendu, on peut remplacer dans cet exemple le nombre $\sqrt{2}$ par une racine carrée de tout nombre rationnel, à condition que cette racine carrée ne soit pas un élément du champ des nombres rationnels. Ainsi, les nombres de la forme $a + bi$ avec a et b rationnels forment un champ.

§ 44. Anneau

Dans plusieurs branches des mathématiques, ainsi que dans les applications des mathématiques en technique et aux sciences naturelles, on rencontre souvent des situations où les opérations algébriques sont appliquées non pas aux nombres, mais à des êtres de nature toute différente. Un grand nombre d'exemples de ce genre se trouvent dans les chapitres précédents de ce livre ; il suffit de rappeler la multiplication et l'addition des matrices, l'addition des vecteurs, les opérations sur les polynômes, ainsi que les opérations sur les applications linéaires. On donne ci-dessous la définition générale d'une *opération algébrique* (qui est valable pour la multiplication et l'addition dans les anneaux numériques et pour les opérations dans les exemples ci-dessus).

Soit un ensemble M qui se compose de nombres, ou bien d'êtres de nature géométrique, ou, plus généralement, d'êtres de nature quelconque, appelés *éléments* de l'ensemble M. Une *opération algébrique est définie sur l'ensemble M* si à *tout* couple d'éléments a et b de M on fait correspondre, d'après une loi donnée, un élément c, bien défini, de l'ensemble M. On peut appeler cette opération *addition*, alors l'élément c est dit *somme* des éléments a et b et est noté : $c = a + b$; cette opération peut s'appeler *multiplication* ; alors c est dit *produit* des éléments a et b et est noté : $c = ab$; enfin, une autre terminologie et d'autres notations sont possibles pour introduire cette opération sur l'ensemble M.

Sur chaque anneau numérique deux opérations indépendantes sont définies — addition et multiplication. En ce qui concerne la soustraction et la division, elles ne sauraient pas être considérées comme des opérations indépendantes, car elles sont inverses, respectivement, de l'addition et de la multiplication, à condition, évidemment, que l'on admette la définition suivante de l'*opération inverse*.

Soit une opération algébrique définie sur l'ensemble M, par exemple l'addition. On dit que *cette opération possède une opération inverse* (ou encore qu'elle est inversible) dite *soustraction* si pour

tout couple d'éléments a et b il existe un élément *unique* d tel que l'égalité suivante soit satisfaite: $b + d = a$. L'élément d, noté $d = a - b$, est dit *différence* des éléments a et b.

Il est clair que les deux opérations, l'addition et la multiplication, définies sur les champs numériques, sont inversibles (il est vrai que pour la multiplication on a une condition: le diviseur doit être non nul). Dans les anneaux numériques qui ne sont pas des champs (par exemple, l'anneau des nombres entiers) il n'y a que l'addition qui soit inversible.

D'autre part, deux opérations algébriques, l'addition et la multiplication, sont aussi définies sur l'ensemble des polynômes d'une indéterminée x à coefficients dans un champ numérique P; en outre, l'addition a pour opération inverse la soustraction.

On sait que l'addition et la multiplication, définies sur un anneau numérique ou sur l'ensemble des polynômes, jouissent des propriétés suivantes (ici a, b, c sont des éléments quelconques de l'anneau numérique donné ou de l'ensemble des polynômes considéré):

I. L'addition est commutative: $a + b = b + a$.

II. L'addition est associative: $a + (b + c) = (a + b) + c$.

III. La multiplication est commutative: $ab = ba$.

IV. La multiplication est associative: $a(bc) = (ab)c$.

V. L'addition et la multiplication sont liées par la loi de distributivité:

$$(a + b)c = ac + bc.$$

Nous sommes maintenant prêts à introduire la notion générale d'anneau, qui est une des notions fondamentales de l'algèbre.

Un ensemble R est appelé *anneau* si deux opérations indépendantes, dites addition et multiplication, sont définies sur cet ensemble; ces opérations sont commutatives, associatives et liées l'une à l'autre par la loi de distributivité; en outre, l'addition est inversible et a pour opération inverse la soustraction.

Ainsi, les anneaux numériques et les anneaux des polynômes d'une indéterminée x à coefficients dans un champ numérique donné P (et même à coefficients dans un anneau numérique donné) sont des exemples concrets d'anneaux. Donnons encore un exemple montrant toute la généralité de cette notion.

Le cours d'analyse débute par l'introduction de la notion de *fonction* d'une variable réelle x. Considérons l'ensemble des fonctions à valeurs réelles, définies pour *toutes* les valeurs réelles de la variable x; définissons sur cet ensemble les opérations algébriques de la manière suivante: la fonction, notée $f(x) + g(x)$, est appelée *somme* des fonctions $f(x)$ et $g(x)$ si pour tout $x = x_0$ la valeur de cette fonction est la somme des valeurs correspondantes des fonctions $f(x)$ et $g(x)$, c'est-à-dire qu'elle est égale à la somme $f(x_0) + g(x_0)$;

la fonction, notée $f(x)\ g(x)$, est appelée *produit* des fonctions $f(x)$ et $g(x)$ si pour tout $x = x_0$ elle est égale au produit $f(x_0) \cdot g(x_0)$. Il est clair que la somme et le produit existent pour tout couple de fonctions de l'ensemble considéré. On vérifie sans peine que les propriétés I-V sont satisfaites dans ce cas, car l'addition et la multiplication des fonctions se réduisent aux opérations correspondantes sur leurs valeurs pour tout x fixé, c'est-à-dire aux opérations correspondantes sur les nombres réels, pour lesquels les propriétés I-V ont manifestement lieu. Enfin, définissant la *différence* de deux fonctions $f(x)$ et $g(x)$ comme une fonction dont la valeur pour tout $x = x_0$ est égale à la différence $f(x_0) - g(x_0)$, nous sommes conduits à la définition de la soustraction, opération inverse de l'addition. Ceci démontre que *l'ensemble des fonctions, définies pour tout x réel, devient un anneau après l'introduction sur cet ensemble des opérations d'addition et de multiplication de la manière décrite ci-dessus.*

On peut obtenir d'autres exemples d'anneaux de fonctions, si l'on conserve les définitions, données ci-dessus, des opérations sur les fonctions et qu'on considère les fonctions définies, par exemple, seulement pour x positifs, ou bien seulement pour x appartenant au segment $[0, 1]$. Plus généralement, l'ensemble des fonctions définies dans un domaine quelconque est un anneau. On peut obtenir d'autres exemples d'anneaux, en ne considérant que les fonctions définies et continues dans un domaine, ces fonctions faisant l'objet d'étude du cours d'analyse. On pourrait, d'autre part, considérer les fonctions à valeurs complexes d'une variable complexe. En général, il existe de nombreux anneaux différents dont les éléments sont des fonctions ou des nombres.

Passons maintenant à l'étude des propriétés les *plus simples* des anneaux, qui découlent directement de leur définition. Dans le cas des nombres le lecteur s'est déjà familiarisé avec ces propriétés, mais il sera peut-être surpris de constater qu'elles résultent uniquement des propriétés I-V et de l'existence de la soustraction bien définie.

D'abord, quelques remarques sur la signification des conditions I-V. Le rôle de la *commutativité* n'a pas besoin d'être expliqué. La signification de l'*associativité* est la suivante: on définit les opérations algébriques, somme et produit, seulement pour un couple d'éléments. Essayant de définir, par exemple, le produit de trois éléments a, b, c, nous nous heurtons au problème suivant: les produits $a \cdot u$ et $v \cdot c$, avec $bc = u$ et $ab = v$, peuvent, dans le cas général, être différents, c'est-à-dire il peut arriver que $a(bc) \neq (ab)c$. La loi d'associativité exige que ces deux produits soient égaux à un même élément de l'anneau; il est naturel de considérer cet élément comme le produit abc, écrit sans parenthèses. En plus, l'*associativité permet de définir d'une façon unique le produit*

(*respectivement la somme*) *d'un nombre fini quelconque d'éléments d'un anneau*, c'est-à-dire elle permet de démontrer que le produit de n éléments ne dépend pas de la manière dont on a mis, dès le début, les parenthèses.

Démontrons cette proposition par récurrence sur n. Pour $n = 3$ elle est déjà démontrée ; soit $n > 3$ et faisons l'hypothèse de récurrence selon laquelle pour tout nombre de facteurs inférieur à n notre proposition soit vraie. Soient n éléments $a_1, a_2, \ldots, a_n$; supposons qu'on ait mis les parenthèses d'une manière quelconque indiquant l'ordre des multiplications que nous avons à effectuer. Le dernier pas est la multiplication du produit des k premiers éléments $a_1a_2 \ldots a_k$ (avec $1 \leqslant k \leqslant n - 1$) par le produit $a_{k+1}a_{k+2} \ldots a_n$. Ces produits ayant des facteurs en nombre inférieur à n, ils sont bien définis, d'après l'hypothèse de récurrence; alors il nous reste seulement à démontrer l'égalité

$$(a_1a_2 \ldots a_k)(a_{k+1}a_{k+2} \ldots a_n) = \\ = (a_1a_2 \ldots a_l)(a_{l+1}a_{l+2} \ldots a_n)$$

pour tous les entiers k et l $(1 \leqslant k,\ l \leqslant n)$. Il suffit, pour cela, de considérer le cas $l = k + 1$.

Or, posant dans ce cas

$$a_1a_2 \ldots a_k = b, \qquad a_{k+2}a_{k+3} \ldots a_n = c,$$

nous obtenons, en vertu de l'associativité, l'égalité

$$b(a_{k+1}c) = (ba_{k+1})c.$$

Ceci démontre notre proposition.

En particulier, on peut parler du produit de n éléments égaux à un même élément, c'est-à-dire on peut introduire la notion de *puissance* $n^{\text{ème}}$ d'un élément a, où n est un entier positif. Il est facile de vérifier que dans chaque anneau les règles ordinaires sont valables pour les opérations sur les puissances. Soit a un élément d'un anneau ; alors l'associativité de l'addition conduit de la même manière à la notion de *multiples* de l'élément a : na, où n est un coefficient entier positif.

La *loi de distributivité*, c'est-à-dire la règle qui consiste à ouvrir les parenthèses, est l'unique restriction dans la définition des anneaux qui établit le rapport entre l'addition et la multiplication; c'est uniquement grâce à cette loi que l'étude commune de ces deux opérations est plus fructueuse que leur étude séparée. Dans l'énoncé de la loi de distributivité la somme ne comprend que deux termes. Toutefois, on démontre facilement que pour tout k l'égalité suivante a lieu

$$(a_1 + a_2 + \ldots + a_k)b = a_1b + a_2b + \ldots + a_kb$$

et on en déduit la règle générale de multiplication de deux sommes.

Quel que soit l'anneau, la loi de distributivité a également lieu pour la différence. En effet, d'après la définition de la différence, l'élé-

ment $a - b$ vérifie l'égalité

$$b + (a - b) = a.$$

Multipliant les deux membres de cette égalité par c et appliquant au premier membre la loi de distributivité, nous obtenons :

$$bc + (a - b)\,c = ac.$$

Donc, l'élément $(a - b)\,c$ est la différence des éléments ac et bc:

$$(a - b)\,c = ac - bc.$$

Des propriétés assez importantes des anneaux peuvent être établies grâce à l'opération de soustraction. Si a est un élément d'un anneau R, alors la différence $a - a$ est un élément bien déterminé de cet anneau. Son rôle est analogue à celui de l'élément nul dans les anneaux numériques ; cependant cet élément, comme on le voit de sa définition, peut dépendre du choix de l'élément a, c'est pourquoi nous le notons par 0_a.

Montrons qu'en réalité les éléments 0_a coïncident pour tous les a. En effet, soit b un élément de l'anneau R ; ajoutant l'élément 0_a aux deux membres de l'égalité

$$a + (b - a) = b$$

et utilisant la relation $0_a + a = a$, il vient

$$0_a + b = 0_a + a + (b - a) = a + (b - a) = b.$$

Ainsi, $0_a = b - b = 0_b$.

Nous avons démontré que *tout anneau R possède un élément bien défini, tel que la somme de cet élément et d'un élément quelconque a de R est égale à l'élément a*. Cet élément, noté 0, est appelé *élément nul* de l'anneau R ; il n'y a pas de danger sérieux de le confondre avec le nombre zéro. Ainsi,

$$a + 0 = a \text{ pour tout } a \text{ de } R.$$

Ensuite, *tout élément a d'un anneau possède un élément opposé bien défini, noté $-a$, qui vérifie l'égalité*

$$a + (-a) = 0,$$

à savoir l'élément opposé à a est défini par la formule: $-a = 0 - a$; l'unicité de l'élément opposé découle de l'unicité de la différence. Il est clair que $-(-a) = a$. Maintenant la différence $b - a$ de deux éléments d'un anneau peut être récrite sous la forme

$$b - a = b + (-a).$$

En effet,

$$[b + (-a)] + a = b + [(-a) + a] = b + 0 = b.$$

Pour tout élément a d'un anneau et pour tout entier positif n on a l'égalité

$$n(-a) = -(na).$$

En effet, groupant les termes il vient :

$$na + n(-a) = n[a + (-a)] = n \cdot 0 = 0.$$

Maintenant nous avons la possibilité de définir les *multiples négatifs* de tout élément a d'un anneau: pour $n > 0$ ce sont les éléments égaux $n(-a)$ et $-(na)$, que nous désignerons par $(-n)a$. Enfin, convenons de considérer comme *multiple* d'un élément *a avec le coefficient nul*, soit $0 \cdot a$, l'élément nul de l'anneau donné.

La définition de l'élément nul est donnée au moyen de l'addition et de son opération inverse, c'est-à-dire sans utiliser la multiplication. Or, dans le cas de la multiplication des nombres, le zéro jouit d'une propriété très importante. Il se révèle que cette même propriété est propre à l'élément nul de tout anneau, notamment *dans chaque anneau le produit de l'élément nul et d'un élément quelconque de cet anneau est l'élément nul.* La démonstration découle directement de la loi de distributivité: soit a un élément d'un anneau R ; alors, quel que soit l'élément auxiliaire x de R, on a

$$a \cdot 0 = a(x - x) = ax - ax = 0.$$

Utilisant cette propriété de l'élément nul on peut démontrer que *pour tout couple d'éléments a et b d'un anneau l'égalité suivante est vraie* :

$$(-a)b = -ab.$$

En effet,

$$ab + (-a)b = [a + (-a)]b = 0 \cdot b = 0.$$

Il s'ensuit que la règle (bien connue, quoique mystérieuse) de multiplication des nombres négatifs: « moins multiplié par moins donne plus », est une conséquence directe de la définition des anneaux ; autrement dit, *pour tout couple d'éléments a et b d'un anneau on a l'égalité*

$$(-a)(-b) = ab.$$

En effet,

$$(-a)(-b) = -[a(-b)] = -(-ab) = ab.$$

Maintenant le lecteur n'aura aucune peine à démontrer que les règles ordinaires sont valables pour les opérations sur les multiples, positifs et négatifs, de tout élément d'un anneau.

Ainsi, les opérations algébriques sur un anneau jouissent d'un grand nombre de propriétés auxquelles nous sommes déjà habitués dans le cas des opérations analogues sur les nombres. Toutefois, il

ne faut pas croire que toute propriété de l'addition ou de la multiplication des nombres est conservée dans un anneau. Ainsi, la multiplication des nombres possède une propriété réciproque à celle citée ci-dessus: *si le produit de deux nombres est nul, alors l'un des facteurs est nul.* Or, cette propriété ne saurait pas être généralisée au cas d'un anneau quelconque, car il existe des anneaux dans lesquels il y a des couples d'éléments tels que leur produit est l'élément nul, tandis qu'aucun facteur ne l'est, c'est-à-dire $a \neq 0$, $b \neq \neq 0$, mais $ab = 0$; ces éléments sont dits *diviseurs de zéro.*

Bien entendu, il n'existe pas d'anneaux numériques ayant des diviseurs de zéro. Les anneaux des polynômes à coefficients numériques n'en possèdent pas non plus. Remarquons d'abord que l'élément nul dans un anneau de fonctions est la fonction identiquement nulle en x. Maintenant, soient deux fonctions $f(x)$ et $g(x)$, définies pour toute valeur réelle de x par les égalités:

$$f(x)=0 \quad \text{pour} \quad x\leqslant 0, \qquad f(x)=x \quad \text{pour} \quad x>0;$$
$$g(x)=x \quad \text{pour} \quad x\leqslant 0, \qquad g(x)=0 \quad \text{pour} \quad x>0.$$

Les deux fonctions sont différentes de l'élément nul de l'anneau considéré car elles ne sont pas identiquement nulles; toutefois leur produit est égal à l'élément nul.

Ce n'est pas toutes les conditions I-V qui sont, dans une mesure égale, nécessaires pour la définition d'un anneau. Le développement des mathématiques montre que les propriétés I et II de l'addition et la loi de distributivité V ont lieu dans tous les exemples, mais qu'il n'en est pas de même pour les conditions III et IV de la multiplication qui sont trop gênantes et limitent le domaine d'application de la notion d'anneau. Ainsi, l'ensemble des matrices carrées d'ordre n à éléments réels, muni des opérations d'addition et de multiplication des matrices, vérifie toutes les conditions de la définition d'un anneau, excepté la loi de commutativité de la multiplication. On rencontre une multiplication non commutative si souvent et dans des cas tellement importants que, actuellement, la notion d'anneau signifie, en règle générale, un *anneau non commutatif* (plus précisément, un anneau n'est pas forcément muni de la multiplication commutative), tandis qu'on appelle *anneaux commutatifs* le type spécial d'anneaux où la condition III est vérifiée.

Dernièrement, les anneaux à multiplication non associative ont suscité un grand intérêt, de sorte que la théorie générale des anneaux se développe, à présent, comme une théorie non associative des anneaux (c'est-à-dire la multiplication n'est plus forcément associative). Le plus simple exemple d'anneaux de ce genre est l'ensemble des vecteurs d'un espace euclidien à trois dimensions muni de l'addition ordinaire et de la multiplication vectorielle, connue du lecteur du cours de géométrie analytique.

§ 45. Champ

De même que nous avons dégagé et appelé champs numériques les anneaux numériques dans lesquels on peut effectuer la division par les éléments non nuls, il est naturel d'introduire de cette manière

la notion de champ dans le cas général. Notons d'abord que, en vertu de la propriété de l'élément nul par rapport à la multiplication, *il n'existe pas d'anneaux où l'on puisse diviser par l'élément nul*; en effet, diviser un élément a par l'élément nul, c'est trouver un élément x tel que $0 \cdot x = a$; or, cette égalité est impossible si $a \neq 0$, le premier membre étant égal à l'élément nul.

Introduisons la définition suivante:

Un anneau P est appelé *champ* s'il contient d'autres éléments que l'élément nul et si on peut diviser tout élément de P par l'élément non nul, le résultat de la division étant bien défini, c'est-à-dire si pour deux éléments a et b de P, où b *est non nul*, il existe dans P un élément unique q tel que l'égalité $bq = a$ soit satisfaite. L'élément q est dit *quotient* de la division de a par b et il est noté $q = \frac{a}{b}$ [1].

Bien entendu, les champs numériques sont des exemples de champs. L'anneau des polynômes d'une indéterminée x à coefficients réels ou, plus généralement, à coefficients appartenant à un champ numérique donné, n'est pas un champ, car la division des polynômes avec reste n'est pas la même chose que la division exacte, imposée dans la définition d'un champ. D'autre part, il est facile de voir que l'*ensemble des fractions rationnelles à coefficients réels* (cf. § 25) *est un champ* contenant l'anneau des polynômes, tout comme le champ des nombres rationnels contient l'anneau des nombres entiers.

En partant des anneaux de fonctions on peut indiquer d'autres exemples de champs; nous ne les donnerons pas ici et passerons à des exemples de tout autre nature.

Les anneaux numériques, ainsi que tous les anneaux que nous avons considérés jusqu'ici, contenaient une infinité d'éléments. Mais il existe des anneaux, voire des champs, composés d'un nombre fini d'éléments. Les plus simples exemples d'*anneaux* et de *champs finis*, utilisés par une branche spéciale des mathématiques, la théorie des nombres, peuvent être construits de la manière suivante.

Soit un nombre entier positif n différent de l'unité. Deux nombres entiers positifs a et b sont dits *équivalents modulo n*,

$$a \equiv b \pmod{n},$$

si la division de ces nombres par n donne le même reste ou, encore, si leur différence est divisible par n. Alors l'anneau des nombres entiers est la réunion de n classes résiduelles modulo n disjointes:

$$C_0, C_1, \ldots, C_{n-1}, \tag{1}$$

---

[1] L'unicité du quotient ainsi que celle de la différence, supposée ci-dessus dans la définition d'un anneau, peuvent être aisément établies en partant d'autres conditions de la définition d'un champ (respectivement d'un anneau).

où la classe C_k est l'ensemble des nombres entiers qui, divisés par n, donnent pour reste le nombre k, $k = 0, 1, \ldots, n - 1$. Il s'avère qu'on peut définir de façon naturelle l'addition et la multiplication des classes (1).

Pour cela choisissons deux classes quelconques C_k et C_l (pas forcément distinctes) de l'ensemble (1). Additionnant un nombre de C_k et un nombre de C_l, nous obtenons un nombre appartenant à une classe bien déterminée, à savoir à la classe C_{k+l} si $k + l < n$, ou bien à la classe C_{k+l-n} si $k + l \geqslant n$. Cela nous conduit à la définition suivante de l'*addition des classes*:

$$\begin{aligned} C_k + C_l &= C_{k+l} \quad \text{si} \quad k+l<n, \\ C_k + C_l &= C_{k+l-n} \quad \text{si} \quad k+l \geqslant n. \end{aligned} \tag{2}$$

D'autre part, en multipliant un nombre de la classe C_k par un nombre de la classe C_l, nous obtenons un nombre qui appartient à une classe bien déterminée, à savoir à la classe C_r, où r est le reste de la division de kl par n. Nous adoptons, donc, la définition suivante pour la *multiplication des classes*:

$$C_k \cdot C_l = C_r \quad \text{avec} \quad kl = nq + r, \qquad 0 \leqslant r < n. \tag{3}$$

L'ensemble (1) *des classes de nombres entiers équivalents modulo n muni des opérations* (2) *et* (3) *forme un anneau.* En effet, les conditions I-V de la définition d'un anneau sont satisfaites, ce qu'on peut vérifier directement; mais il faut mentionner que ces conditions découlent également des propriétés analogues de l'anneau des nombres entiers et du lien établi ci-dessus entre les opérations sur les nombres entiers et celles sur les classes C_k. Il est clair que la classe C_0, composée des nombres entiers divisibles par n, joue le rôle de l'élément nul. Une classe C_k a pour opposée la classe C_{n-k}, $k = 1, 2, \ldots, n - 1$. Par conséquent, on peut définir la soustraction des classes de l'ensemble (1), c'est-à-dire cet ensemble vérifie toutes les conditions de la définition d'un anneau. Convenons de désigner cet anneau par Z_n.

Si l'entier n n'est pas un nombre premier, l'anneau Z_n possède des diviseurs de zéro (on montrera plus tard que, pour cette raison, Z_n ne peut pas être un champ). En effet, si $n = kl$ avec $1 < k < n$, $1 < l < n$, les classes non nulles C_k et C_l, en vertu de la définition (3), donnent après leur multiplication la classe nulle C_0 : $C_kC_l = C_0$.

Si l'entier n est un nombre premier, alors l'anneau Z_n est un champ.

En effet, soient deux classes C_k et C_m, où $C_k \neq C_0$, c'est-à-dire $1 \leqslant k \leqslant n - 1$. Il faut montrer que la classe C_m peut être divisée par la classe C_k, c'est-à-dire il faut trouver une classe C_l telle que l'on ait: $C_k \cdot C_l = C_m$. Si $C_m = C_0$, alors $C_l = C_0$.

Supposons que $C_m \neq C_0$ et considérons l'ensemble des entiers

$$k,\ 2k,\ 3k,\ \ldots,\ (n-1)k. \qquad (4)$$

Aucun de ces nombres n'appartient à la classe C_0, le produit de deux entiers ne pouvant pas être divisible par un nombre premier si chaque facteur est inférieur au diviseur. Puis, deux nombres sk et tk, $s < t$, de l'ensemble (4) appartiennent à des classes distinctes, car leur différence

$$tk - sk = (t-s)\,k$$

ne peut pas être divisible par n, le nombre n étant premier. Ainsi, toute classe non nulle contient exactement un élément de l'ensemble (4). En particulier, la classe C_m contient le nombre lk, où $1 \leqslant l \leqslant n-1$, ce qui signifie que $C_l \cdot C_k = C_m$, c'est-à-dire la classe C_l est le quotient cherché de la division de C_m par C_k.

Ainsi, nous obtenons une infinité de champs finis différents: le champ Z_2 (composé seulement de deux éléments), les champs Z_3, Z_5, Z_7, Z_{11}, etc.

Passons à l'étude de *certaines propriétés des champs*, qui découlent de l'existence de la division. Elles sont analogues aux propriétés correspondantes des anneaux qui résultent de l'existence de la soustraction et peuvent être démontrées par les mêmes raisonnements, de sorte que nous laissons au lecteur le soin de les vérifier.

Tout champ P possède un élément unique qui, multiplié par tout élément a de P, donne l'élément a. Cet élément, noté 1 et égal à tous les quotients $\frac{a}{a}$, avec a non nul, est dit élément *unité* (ou unité tout court) du champ P. Ainsi, on a

$$a \cdot 1 = a \text{ pour tout } a \text{ de } P.$$

Pour tout élément a non nul il existe dans un champ P un élément inverse bien défini, noté a^{-1}, qui vérifie l'égalité

$$a \cdot a^{-1} = 1\,;$$

notamment, $a^{-1} = \frac{1}{a}$. Il est clair que $(a^{-1})^{-1} = a$. A présent, le quotient $\frac{b}{a}$ peut être récrit sous la forme

$$\frac{b}{a} = b \cdot a^{-1}$$

Pour tout élément a non nul et pour tout entier positif n l'égalité

$$(a^{-1})^n = (a^n)^{-1}$$

a lieu. Désignant par a^{-n} ces deux éléments égaux, nous sommes conduits à la définition des *puissances d'exposants entiers négatifs* d'un

élément non nul d'un champ; en outre, les règles ordinaires d'opérations sur les puissances sont valables. Enfin, posons pour tout a : $a^0 = 1$.

L'existence d'une unité n'est pas une propriété caractéristique des champs, l'anneau des nombres entiers, par exemple, en possédant une également. D'autre part, l'exemple fourni par l'anneau des nombres pairs montre que ce n'est pas tous les anneaux qui ont une unité. Mais, *tout anneau possédant une unité et contenant avec un élément a non nul son inverse a^{-1} est un champ.* En effet, dans ce cas le quotient $\frac{b}{a}$, $a \neq 0$, est défini par la formule : $\frac{b}{a} = ba^{-1}$. L'unicité de ce quotient se démontre facilement.

Remarquons que *dans un champ il n'existe pas de diviseurs de zéro.* En effet, supposons le contraire : $ab = 0$, mais $a \neq 0$. Multipliant les deux membres de cette égalité par l'élément a^{-1}, nous obtenons dans le premier membre : $(a^{-1}a)\, b = 1 \cdot b = b$, et dans le second : $a^{-1} \cdot 0 = 0$, c'est-à-dire $b = 0$. Il en résulte que *dans un champ toute égalité peut être simplifiée en la divisant par le facteur commun non nul.* En effet, soit $ac = bc$ avec $c \neq 0$; alors $(a - b)\, c = 0$, d'où l'on a $a - b = 0$ ou encore $a = b$.

On déduit aisément de la définition d'un quotient $\frac{a}{b}$ $(b \neq 0)$ et de la formule $\frac{a}{b} = a \cdot b^{-1}$, établie ci-dessus, que les *règles ordinaires d'opérations sur les fractions sont conservées dans un champ*, notamment,

$$\frac{a}{b} = \frac{c}{d} \text{ si et seulement si } ad = bc;$$

$$\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd};$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$

$$\frac{-a}{b} = -\frac{a}{b}.$$

Caractéristique d'un champ. Ce n'est pas toutes les propriétés des champs numériques qui sont conservées dans un champ quelconque. Ainsi, additionnant le nombre 1 un certain nombre de fois, c'est-à-dire formant les multiples du nombre 1 avec les coefficients entiers positifs, nous n'obtenons jamais zéro; en outre, tous ces multiples, qui constituent l'ensemble des nombres entiers positifs, sont des éléments distincts. Or, les multiples positifs de l'unité dans un champ fini ne peuvent pas être tous distincts, car il n'y a qu'un nombre fini d'éléments dans le champ considéré. Si un champ P est tel que tous les multiples de l'unité sont des éléments distincts de P, c'est-à-dire $k \cdot 1 \neq l \cdot 1$ pour $k \neq l$, alors P est dit

champ *de caractéristique nulle* ; tels sont, par exemple, tous les champs numériques. Si, par contre, il existe deux entiers k et l tels que $k > l$, mais $k \cdot 1 = l \cdot 1$ dans P, alors $(k - l) \cdot 1 = 0$, c'est-à-dire il existe dans P un multiple positif de l'unité qui est égal à l'élément nul de P. Dans ce cas P est dit champ *de caractéristique finie*, notamment, *de caractéristique p* si p est le premier coefficient entier positif tel que $p \cdot 1 = 0$ dans P. Les champs finis sont des exemples de champs de caractéristique finie ; il existe, d'ailleurs, des champs infinis ayant la caractéristique finie.

Si un champ P est de caractéristique p, alors p est un nombre premier.

En effet, supposant que $p = st$ avec $s < p$, $t < p$, nous serions conduits à l'égalité $(s \cdot 1)(t \cdot 1) = p \cdot 1 = 0$, ou encore, vu que dans un champ il n'existe pas de diviseurs de zéro, on aurait soit l'égalité $s \cdot 1 = 0$, soit l'égalité $t \cdot 1 = 0$, ce qui est en contradiction avec la définition d'une caractéristique en tant que *plus petit* coefficient entier positif, qui, multiplié par l'unité, donne l'élément nul.

Si p est la caractéristique d'un champ P, alors pour tout élément a de P on a l'égalité: $pa = 0$. *Si la caractéristique d'un champ P est nulle, alors pour tout élément a de P et pour tout entier n les inégalités* $a \neq 0$ *et* $n \neq 0$ *entraînent*: $na \neq 0$.

En effet, dans le premier cas l'élément pa, somme de p termes égaux à a, peut être représenté, en mettant a en facteur, sous la forme

$$pa = a(p \cdot 1) = a \cdot 0 = 0.$$

Dans le second cas, l'égalité $na = 0$ ou, encore, $a(n \cdot 1) = 0$ aurait pour conséquence l'égalité $n \cdot 1 = 0$, car $a \neq 0$; la caractéristique du champ P étant nulle, il en résulterait que $n = 0$.

Sous-champs, extensions. Supposons qu'un sous-ensemble P' de l'ensemble des éléments d'un champ P soit, lui aussi, un champ par rapport aux opérations définies dans le champ P, c'est-à-dire que pour tout couple d'éléments a et b de P', les éléments $a + b$, ab, $a - b$ et $\frac{a}{b}$ (avec $b \neq 0$), qui appartiennent au champ P, soient, en même temps, des éléments de P' (les conditions I-V étant satisfaites dans P, elles sont également vraies pour P'). Alors, P' est dit *sous-champ* du champ P, tandis que P s'appelle *extension* du champ P'. Bien entendu, l'élément nul et l'unité du champ P appartiennent également à P' et sont, respectivement, l'élément nul et l'unité de P'. Ainsi, le champ des nombres rationnels est un sous-champ du champ des nombres réels ; tout champ numérique est un sous-champ des nombres complexes.

Soient P' un sous-champ d'un champ P et c un élément de P qui n'appartient pas à P' ; supposons que nous ayons trouvé un sous-

champ minimal P'' de P contenant P' et c. Un tel sous-champ minimal est défini de façon unique, car s'il existait encore un sous-champ P''' ayant ces propriétés, alors l'intersection des sous-champs P'' et P''' (c'est-à-dire la partie commune de ces sous-champs) contiendrait P' et l'élément c; en outre, pour tout couple d'éléments de l'intersection, la somme, le produit, la différence et le quotient étant des éléments de P'' et de P''', ils appartiendraient également à l'intersection de P'' et de P'''; autrement dit, cette intersection serait, elle aussi, un sous-champ, ce qui contredit l'hypothèse que le sous-champ P'' est minimal. Nous dirons que le champ P'' *est obtenu par adjonction de l'élément c au champ P'* et nous utiliserons la notation $P'' = P'(c)$.

Il est clair que le champ $P'(c)$ contient, outre c et le champ P', tous les éléments qui s'en obtiennent au moyen des opérations d'addition, de multiplication, de soustraction et de division. Le champ numérique composé des éléments de la forme $a + b\sqrt{2}$ avec a et b rationnels (ce champ a été considéré au § 43) donne un exemple d'extension du champ des nombres rationnels qui s'obtient en adjoignant à ce dernier le nombre $\sqrt{2}$.

§ 46*. Isomorphisme des anneaux (des champs). Unicité du champ des nombres complexes

Dans la théorie des anneaux la notion d'isomorphisme joue un rôle très important. Notamment, deux anneaux L et L' sont dits *isomorphes* s'il existe une application bijective entre les éléments de L et L' telle que pour tout couple d'éléments a et b de L (dont les images dans L' sont respectivement a' et b') l'image de la somme $a + b$ et celle du produit ab sont respectivement $a' + b'$ et $a'b'$.

Supposons que les anneaux L et L' soient isomorphes. Alors, *l'isomorphisme fait correspondre à l'élément nul 0 de L l'élément nul $0'$ de L'.* En effet, soit c' l'image de 0 dans L'. Soient a un élément de L et a' son image dans L'. Alors, à l'élément $a + 0$ correspond l'élément $a' + c'$; or, $a + 0 = a$, de sorte que $a' + c' = a'$, d'où $c' = 0'$. Ensuite *l'élément $-a$ a pour image l'élément $-a'$.* En effet, soit d' l'image de $-a$. Alors, à l'élément $a + (-a) = 0$ correspond l'élément $a' + d'$, c'est-à-dire $a' + d' = 0'$, d'où on a: $d' = -a'$. Il en résulte que la *différence de deux éléments de L a pour image par isomorphisme la différence des images de ces éléments.* Des raisonnements analogues montrent que si un anneau L possède une unité, alors l'image de l'unité par isomorphisme est l'unité de l'anneau L' de même que si un élément a de L est inversible, soit a^{-1} son inverse, alors l'image de a^{-1}, par isomorphisme entre L et L', est l'inverse de l'élément a', image de a.

Il en résulte qu'un *anneau isomorphe à un champ est lui-même un champ.* Il est aussi facile de voir que si un anneau n'a pas de diviseurs de zéro, alors cette propriété est conservée par isomorphisme. Plus généralement, deux anneaux isomorphes peuvent avoir des éléments de nature différente, mais ils sont identiques du point de vue de leurs propriétés algébriques; tout théorème vrai pour un anneau l'est également pour tout anneau isomorphe, à condition que la démonstration de ce théorème n'utilise que les propriétés des opérations algébriques sur l'anneau et non les propriétés intrinsèques des éléments. Pour cette raison *nous ne ferons pas de distinction entre les anneaux et les champs isomorphes* ; ils seront des réalisations concrètes d'un même anneau ou d'un même champ.

Appliquons cette notion au problème de construction du champ des nombres complexes. La méthode d'introduction du champ des nombres complexes exposée au § 17, qui est basée sur l'utilisation des points d'un plan, n'est pas la seule possible. Au lieu des points on aurait pu utiliser les mêmes formules (2) et (3) du § 17 pour définir l'addition et la multiplication des vecteurs. D'ailleurs, nous aurions pu renoncer tout à fait au point de vue géométrique; remarquant que les points et les vecteurs d'un plan sont donnés par des couples ordonnés de nombres réels (a, b), nous aurions pu munir l'ensemble de ces couples ordonnés de l'addition et de la multiplication conformément aux formules (2) et (3) du § 17.

En réalité, tous ces champs seraient identiques du point de vue de leurs propriétés algébriques comme le démontre le théorème suivant:

Toutes les extensions du champ des nombres réels D, qui s'obtiennent par adjonction d'une racine de l'équation

$$x^2+1=0, \tag{1}$$

au champ D sont isomorphes.

En effet, soit un champ P, extension du champ D, qui contient un élément satisfaisant à l'équation (1). Le choix de la notation pour cet élément ne dépend que de nous, et nous utiliserons pour cela la lettre i. Ainsi, nous avons l'égalité: $i^2 + 1 = 0$ (d'où $i^2 = -1$), les puissances et les sommes devant être interprétées du point de vue des opérations définies sur le champ P. Nous voulons trouver le champ $D(i)$ qui s'obtient par adjonction de l'élément i au champ D, c'est-à-dire nous nous proposons de trouver le sous-champ minimal du champ P contenant le champ D et l'élément i.

A ce dessein considérons les éléments α du champ P qui peuvent être mis sous la forme

$$\alpha = a + bi, \tag{2}$$

avec a et b réels: ici le produit du nombre b et de l'élément i, ainsi que la somme du nombre a et de ce produit doivent être interprétés

du point de vue des opérations dans P. Aucun élément α du champ P ne peut avoir deux écritures distinctes (2); en effet, si l'on avait

$$\alpha = a + bi = \bar{a} + \bar{b}i$$

avec $b \neq \bar{b}$, il en découlerait que

$$i = \frac{\bar{a} - a}{b - \bar{b}},$$

c'est-à-dire le nombre i serait réel; or, si $b = \bar{b}$, alors on a $a = \bar{a}$. L'ensemble des éléments du champ P ayant la forme (2) contient, en particulier, tous les nombres réels ($b = 0$) et l'élément i ($a = 0$, $b = 1$).

Montrons que l'*ensemble des éléments qui s'écrivent sous la forme* (2) *est un sous-champ du champ P*; ce sous-champ est le champ cherché $D(i)$. Soient deux éléments $\alpha = a + bi$ et $\beta = c + di$. Alors, tenant compte de la commutativité et de l'associativité de l'addition et de la loi de distributivité qui ont lieu dans le champ P, nous obtenons:

$$\alpha + \beta = (a + bi) + (c + di) = (a + c) + (bi + di),$$

d'où

$$\alpha + \beta = (a + c) + (b + d)\,i, \tag{3}$$

c'est-à-dire cette somme appartient encore à l'ensemble considéré. Ensuite, on a

$$-\beta = (-c) + (-d)\,i,$$

car, d'après (3), nous avons dans ce cas l'égalité: $\beta + (-\beta) = 0 + 0 \cdot i = 0$; ainsi,

$$\alpha - \beta = \alpha + (-\beta) = (a - c) + (b - d)\,i, \tag{3'}$$

c'est-à-dire la différence de deux éléments de l'ensemble considéré est encore un élément de cet ensemble. Utilisant de nouveau les propriétés I-V qui sont satisfaites pour les opérations dans le champ P (cf. § 44) et tenant compte de l'égalité $i^2 = -1$, il vient:

$$\alpha\beta = (a + bi)(c + di) = ac + adi + bci + bdi^2,$$

ou, encore,

$$\alpha\beta = (ac - bd) + (ad + bc)\,i; \tag{4}$$

ainsi, le produit de tout couple d'éléments de la forme (2) est encore un élément de la même forme. Enfin, supposons que $\beta \neq 0$, c'est-à-dire que soit $c \neq 0$, soit $d \neq 0$. Alors, il en est de même pour $c - di$: $c - di \neq 0$; on a:

$$(c + di)(c - di) = c^2 - (di)^2 = c^2 - d^2 i^2 = c^2 + d^2,$$

avec $c^2 + d^2 \neq 0$. Ainsi, en vertu de la proposition du paragraphe précédent d'après laquelle les règles ordinaires d'opérations sur les fractions sont conservées dans tout champ (et, en particulier, une fraction conserve sa valeur lorsqu'on multiplie son numérateur et son dénominateur par un même élément non nul), nous obtenons:

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)\,i}{c^2+d^2},$$

c'est-à-dire l'élément

$$\frac{\alpha}{\beta} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i \tag{4'}$$

est encore de la forme (2).

Montrons maintenant que le *sous-champ obtenu $D(i)$ du champ P est isomorphe au champ des points du plan construit au* § 17. Faisant correspondre à tout élément $a + bi$ du champ $D(i)$ le point (a, b), nous établissons, en vertu de l'unicité de l'écriture (2) montrée ci-dessus, une application bijective entre les éléments du champ $D(i)$ et les points du plan. En outre, à un nombre réel a, en vertu de l'égalité $a = a + 0i$, correspond le point $(a, 0)$, tandis que l'élément $i = 0 + 1\cdot i$ a pour image le point $(0, 1)$. D'autre part, comparant les formules (3) et (4) du paragraphe présent avec les formules (2) et (3) du § 17, nous voyons qu'à la somme et au produit de deux éléments α et β du champ $D(i)$ correspondent les points du plan qui sont respectivement somme et produit des points images de α et de β.

Deux champs isomorphes à un troisième étant aussi isomorphes, la démonstration du théorème est achevée. En particulier, on voit que le choix des formules (2) et (3) du § 17 pour la définition des opérations sur les points n'était pas fortuit et ne peut pas être modifié.

Outre les définitions du champ des nombres complexes considérées ci-dessus, il existe beaucoup d'autres méthodes d'introduction de ce champ. Voici l'une d'elles qui utilise l'addition et la multiplication des matrices.

Considérons l'anneau non commutatif des matrices d'ordre deux sur le champ des nombres réels. Il est clair que les matrices scalaires

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

forment un sous-champ dans cet anneau, ce sous-champ étant isomorphe au champ des nombres réels. Il s'avère que *dans l'anneau des matrices d'ordre deux sur le champ des nombres réels on peut trouver également un sous-champ isomorphe au champ des nombres complexes.* En effet, faisons correspondre à un nombre complexe $a + bi$ la *matrice*

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

De cette façon, nous obtenons une application bijective du champ des nombres complexes sur un sous-ensemble de l'ensemble des matrices d'ordre deux; il

découle des égalités:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}$$

que cette application est un isomorphisme, les matrices dans les seconds membres de ces égalités ayant pour images respectivement les nombres complexes $(a+c)+(b+d)\,i=(a+bi)+(c+di)$ et $(ac-bd)+(ad+bc)\,i=$ $=(a+bi)\,(c+di)$. En particulier, le rôle de l'unité imaginaire i est tenu par la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Le résultat obtenu montre encore une possibilité d introduire le champ des nombres complexes; d'ailleurs, cette méthode est aussi satisfaisante que toutes les autres indiquées ci-dessus.

§ 47. Algèbre linéaire et algèbre des polynômes sur un champ

Dans les chapitres précédents consacrés à l'étude de l'*algèbre linéaire*, le champ des nombres réels jouait le rôle de champ de base. Toutefois, on vérifie aisément que la plupart des résultats de ces chapitres se généralisent sans aucunes modifications au cas d'un champ de base quelconque.

Ainsi, *la méthode de Gauss de résolution des systèmes d'équations linéaires, la théorie des déterminants et les formules de Cramer, exposées dans le chapitre I, sont vraies sur un champ de base P quelconque.*

Il n'y a que la remarque sur les déterminants antisymétriques donnée à la fin du § 4 qui fait supposer que la caractéristique du champ doit être *différente de deux*. D'ailleurs, la démonstration de la propriété 4 de ce même paragraphe n'a plus de vigueur si la caractéristique du champ P est deux, quoique la propriété elle-même reste vraie.

Il est également utile de noter que la proposition relative à l'existence d'une infinité de solutions pour un système indéterminé d'équations linéaires, mentionnée plus d'une fois dans le chapitre I, est vraie pour tout champ *infini* P, mais cesse de l'être si le champ P est *fini*.

Ensuite, *la théorie de la dépendance linéaire des vecteurs, celle du rang d'une matrice et la théorie générale des systèmes d'équations linéaires, exposées dans le chapitre II, ainsi que l'algèbre des matrices du chapitre III, se généralisent au cas d'un champ de base quelconque.*

La théorie générale des formes quadratiques, exposée au § 26, *s'étend au cas d'un champ de base P de caractéristique différente de deux.*

Il est facile de montrer que sans cette dernière restriction le théorème fondamental du § 26 n'est plus vrai.

En effet, soit $P = Z_2$, c'est-à-dire P est le champ composé de deux éléments 0 et 1 ; en outre, $1 + 1 = 0$, d'où on a $-1 = 1$; soit la forme quadratique $f = x_1x_2$ sur le champ P. S'il existe une transformation linéaire

$$x_1 = b_{11}y_1 + b_{12}y_2,$$
$$x_2 = b_{21}y_1 + b_{22}y_2,$$

réduisant f à la forme canonique, alors le coefficient $b_{11}b_{22} + b_{12}b_{21}$, qui précède dans l'égalité

$$f = (b_{11}y_1 + b_{12}y_2)(b_{21}y_1 + b_{22}y_2) =$$
$$= b_{11}b_{21}y_1^2 + (b_{11}b_{22} + b_{12}b_{21})\, y_1y_2 + b_{12}b_{22}y_2^2$$

le produit y_1y_2, doit être nul. Or, ce coefficient est égal au déterminant de la transformation linéaire en question, car dans ce cas $b_{12}b_{21} = -b_{12}b_{21}$ aussi bien pour $b_{12}b_{21} = 1$ que pour $b_{12}b_{21} = 0$. Donc, la transformation linéaire en question est dégénérée.

La suite de l'exposé du chapitre VI dépend essentiellement de ce que l'on considère les formes quadratiques à coefficients réels ou complexes.

Enfin, *la théorie des espaces vectoriels et des applications linéaires sur ces espaces, considérée dans le chapitre* VII, *reste valable pour un champ de base P quelconque*. Seulement, la notion de racine caractéristique est liée à la théorie des polynômes sur un champ quelconque dont il sera question plus tard. Notons que le théorème du § 33 sur le lien entre les racines caractéristiques et les valeurs propres s'énonce à présent de façon suivante : ce ne sont que les racines caractéristiques d'une application linéaire φ appartenant au champ de base P qui sont les valeurs propres de φ.

En ce qui concerne les espaces euclidiens (chapitre VIII) ils sont très étroitement liés au champ des nombres réels.

Certains résultats de l'*algèbre des polynômes* peuvent être étendus au cas d'un champ de base P quelconque. Mais il faut d'abord donner un sens précis à la notion de polynôme sur un champ.

Le problème consiste en ce qu'au § 20 il y a deux points de vue sur la notion de polynôme : le point de vue formellement algébrique et celui de la théorie des fonctions. Ils peuvent être généralisés, tous les deux, au cas d'un champ de base quelconque. Néanmoins, ces deux points de vue étant équivalents dans le cas de champs numériques (cf. § 24) et, plus généralement, dans le cas d'un champ infini (comme il est facile de le vérifier), *ils ne le sont plus dans le cas des champs finis.*

Considérons, par exemple, le champ Z_2, introduit au § 45, qui est composé des deux éléments 0 et 1 ; en outre, $1 + 1 = 0$. Les polynômes $x + 1$ et $x^2 + 1$ à coefficients dans Z_2 sont différents, c'est-à-dire ils ne vérifient pas la condition algébrique d'égalité

de deux polynômes. Toutefois, ces deux polynômes prennent la même valeur 1 pour $x = 0$ et la même valeur 0 pour $x = 1$, c'est-à-dire ces polynômes, en tant que « fonctions » de l'« indéterminée » x du champ Z_2, doivent être considérés comme identiques. Le même phénomène a lieu pour les polynômes $x^3 + x + 1$ et $2x + 1$ sur le champ Z_3, composé des trois éléments 0, 1, 2 ; on a dans Z_3 : $1 + 2 = = 0$. On peut indiquer des exemples de ce genre pour tout champ fini.

Ainsi, une théorie des polynômes sur un champ P quelconque ne saurait être basée sur une définition des polynômes du point de vue de la théorie des fonctions. Donc, il est nécessaire de rendre tout à fait claire la définition formellement algébrique des polynômes. A ce dessein, nous allons donner une *construction de l'anneau des polynômes sur un champ P* qui, dès le début, n'utilise pas l'écriture ordinaire des polynômes au moyen d'une « indéterminée » x.

Considérons l'ensemble des suites finies ordonnées des éléments d'un champ P ayant la forme

$$(a_0, a_1, \ldots, a_{n-1}, a_n), \tag{1}$$

où n est un entier, $n \geqslant 0$; en outre, si $n > 0$, on suppose que $a_n \neq 0$. Munissant l'ensemble des suites (1) des opérations d'addition et de multiplication conformément aux formules (3) et (4) du § 20, nous le transformons en un anneau commutatif ; la démonstration des propriétés correspondantes utilise les mêmes raisonnements que ceux du § 20 dans le cas des polynômes ordinaires.

L'ensemble des suites de la forme (a) (le cas $n = 0$) de l'anneau construit est un sous-champ isomorphe au champ P. Cela permet d'identifier toute suite (a) à l'élément a du champ P, c'est-à-dire on peut poser

$$(a) = a, \text{ pour tout } a \text{ de } P. \tag{2}$$

D'autre part, désignons la suite (0, 1) par la lettre x,

$$x = (0, 1).$$

Alors, la multiplication définie ci-dessus donne : $x^2 = (0, 0, 1)$ et, plus généralement,

$$x^k = (\underbrace{0, 0, \ldots, 0}_{k \text{ fois}}, 1). \tag{3}$$

Utilisant maintenant l'addition et la multiplication des suites ordonnées, définies ci-dessus, ainsi que les égalités (2) et (3), nous

obtenons :

$$(a_0, a_1, a_2, \ldots, a_{n-1}, a_n) = (a_0) + (0, a_1) + (0, 0, a_2) + \ldots$$
$$\ldots + (\underbrace{0, 0, \ldots, 0}_{n-1 \text{ fois}}, a_{n-1}) + (\underbrace{0, 0, \ldots, 0}_{n \text{ fois}}, a_n) =$$
$$= (a_0) + (a_1)(0, 1) + (a_2)(0, 0, 1) + \ldots$$
$$\ldots + (a_{n-1})(\underbrace{0, 0, \ldots, 0}_{n-1 \text{ fois}}, 1) + (a_n)(\underbrace{0, 0, \ldots, 0}_{n \text{ fois}}, 1) =$$
$$= a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + a_nx^n.$$

Ainsi, toute suite ordonnée de la forme (1) peut être écrite sous forme d'un polynôme de x à coefficients dans le champ P ; en outre, il est clair que cette forme d'écriture est unique. Enfin, en s'appuyant sur la commutativité de l'addition, déjà démontrée, on peut passer à la forme d'écriture suivant les puissances décroissantes de x.

Ainsi, nous avons construit un anneau commutatif qu'il est naturel d'appeler *anneau des polynômes d'une indéterminée x sur un champ P*. On le note $P[x]$.

On a déjà montré que l'*anneau $P[x]$ contient le champ P*. Ensuite, tout comme dans le cas d'anneaux des polynômes sur des champs numériques (cf. § 20), l'*anneau $P[x]$ possède un élément unité, il n'a pas de diviseurs de zéro et n'est pas un champ.*

Si un champ P est un sous-champ d'un champ $\overline{P}$, alors l'anneau $P[x]$ est un sous-anneau de l'anneau $\overline{P}[x]$. En effet, tout polynôme à coefficients dans P peut être considéré comme un polynôme sur le champ $\overline{P}$; la somme et le produit de polynômes ne dépendent que de leurs coefficients, de sorte que la somme et le produit se conservent lorsqu'on passe à un champ plus large.

Pour mieux comprendre la notion d'« anneau des polynômes sur un champ P », considérons cette notion d'un autre point de vue.

Supposons que le champ P soit un sous-anneau d'un anneau commutatif L. Un élément α de l'anneau L est dit *algébrique sur le champ P* s'il existe une équation algébrique de degré n, $n \geqslant 1$, à coefficients dans le champ P telle que l'élément α vérifie cette équation ; si, par contre, une telle équation n'existe pas, alors l'élément α est dit *transcendant sur le champ P*. Il est clair que l'élément x de l'anneau $P[x]$ est transcendant sur le champ P.

Le *théorème* suivant est vrai :

Si un élément α d'un anneau L est transcendant sur un champ P, alors le sous-anneau L' obtenu par adjonction de l'élément α au champ P (c'est-à-dire le sous-anneau minimal de l'anneau L, contenant le

champ P et l'élément α) *est isomorphe à l'anneau des polynômes* $P[x]$.

En effet, tout élément β de l'anneau L qui peut être mis sous la forme

$$\beta = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n, \qquad n \geqslant 0, \tag{4}$$

à coefficients $a_0, a_1, \ldots, a_{n-1}, a_n$ dans le champ P, est un élément du sous-anneau L'. Un élément β ne peut pas avoir deux formes (4) distinctes, car, en supposant le contraire et en retranchant l'une des représentations (4) de l'autre, nous obtiendrions une équation algébrique sur le champ P satisfaite par l'élément α, ce qui est contraire à ce que α est transcendant. Additionnant les éléments de la forme (4) d'après les règles d'addition de l'anneau L, nous constatons que cela est équivalent à l'addition des coefficients des mêmes puissances de α; or, c'est là la règle d'addition des polynômes. D'autre part, multipliant les éléments de la forme (4) d'après les règles de multiplication de l'anneau L, on peut, utilisant la loi de distributivité, multiplier terme à terme puis grouper les termes semblables; cela nous conduit évidemment à la règle bien connue de multiplication des polynômes. Cela démontre que les éléments de la forme (4) forment un sous-anneau de l'anneau L, qui contient le champ P et l'élément α, c'est-à-dire qui coïncide avec L', et est isomorphe à l'anneau des polynômes $P[x]$.

Nous voyons que le choix des opérations fait ci-dessus n'est pas arbitraire; il est bien défini par le fait que l'élément x de l'anneau $P[x]$ doit être transcendant sur le champ P.

Notons que la construction de l'anneau des polynômes $P[x]$ n'utilise pas la division des éléments du champ P, et ce n'est qu'une fois, notamment en démontrant la proposition sur le degré du produit de polynômes, qu'on a utilisé l'absence de diviseurs de zéro dans le champ P. Par conséquent, on peut prendre un anneau commutatif quelconque L et, répétant la construction ci-dessus, obtenir l'*anneau des polynômes* $L[x]$ *sur l'anneau* L; *si, de plus, l'anneau* L *n'a pas de diviseurs de zéro*, alors le degré du produit de polynômes est égal à la somme des degrés des facteurs, de sorte que l'*anneau des polynômes* $L[x]$ *ne contient pas, non plus, de diviseurs de zéro.*

Revenant aux polynômes à coefficients dans un champ P, remarquons que la *théorie de la divisibilité des polynômes*, exposée aux §§ 20-22, s'étend, en substance, à ce cas. Notamment, l'*algorithme de division avec reste est valable dans l'anneau* $P[x]$; en outre, aussi bien le quotient que le reste appartiennent à l'anneau $P[x]$.

Ensuite, la *notion de diviseur a un sens dans l'anneau* $P[x]$ *et ses propriétés essentielles sont conservées.* De plus, le fait que l'algorithme de division ne fait pas sortir du champ de base P permet d'affirmer que la *propriété d'un polynôme* $\varphi(x)$ *d'être un diviseur de* $f(x)$ *ne dé-*

pend pas de ce que nous considérons le champ P ou toute extension de P.

La définition et toutes les propriétés du plus grand commun diviseur, y compris l'algorithme d'Euclide et le théorème démontré au § 21 *à l'aide de cet algorithme, sont conservées dans l'anneau $P[x]$.* Remarquons que, en vertu de l'indépendance de l'algorithme de division avec reste du choix d'un champ de base, on peut affirmer que *le plus grand commun diviseur de deux polynômes donnés ne dépend pas non plus de ce que l'on considère le champ P ou une extension quelconque $\overline{P}$.*

Enfin, *pour les polynômes sur un champ P, la notion de zéro a un sens et les propriétés essentielles des zéros sont conservées.* La théorie des zéros multiples est également valable; d'ailleurs nous y reviendrons encore à la fin du paragraphe suivant.

Ces remarques nous permettront, dans l'étude ultérieure des polynômes sur un champ P, de nous référer aux §§ 20-22.

§ 48. Décomposition des polynômes en facteurs irréductibles

En partant du théorème d'existence d'un zéro dans le champ des nombres réels ou des nombres complexes du § 24 nous avons démontré l'existence et l'unicité de la décomposition d'un polynôme en facteurs irréductibles. Ces résultats sont des cas particuliers de théorèmes plus généraux se rapportant aux polynômes sur un champ P quelconque. Ce paragraphe est consacré au développement de cette théorie qui est analogue à celle de la décomposition des nombres entiers en facteurs premiers.

Définissons d'abord les polynômes dont le rôle dans l'anneau des polynômes est analogue à celui des nombres premiers dans l'anneau des nombres entiers. Soulignons dès le début qu'il s'agit dans cette définition des polynômes de *degré supérieur ou égal à l'unité*; ceci est analogue à ce que, en définissant les nombres premiers et en décomposant les nombres entiers en facteurs premiers, les nombres 1 et -1 ne sont pas considérés comme premiers.

Soit un polynôme $f(x)$ de degré n, $n \geqslant 1$, à coefficients dans un champ P. Vu la propriété V du § 21, tout polynôme de degré nul est un diviseur de $f(x)$. D'autre part, d'après VII, tous les polynômes de la forme $cf(x)$, c étant un élément non nul du champ P, sont des diviseurs de $f(x)$; en outre il n'y a pas d'autres diviseurs de $f(x)$ de degré n. En ce qui concerne les diviseurs de $f(x)$ de degrés supérieurs à 0 mais inférieurs à n, ils peuvent exister ou ne pas exister dans l'anneau $P[x]$. Dans le premier cas, le polynôme $f(x)$ est dit *réductible* dans le champ P (ou réductible sur le champ P), et dans le second *irréductible* dans ce champ.

Rappelant la définition d'un diviseur, on peut dire qu'un *polynôme $f(x)$ de degré n est réductible sur un champ P s'il peut être décomposé sur ce champ (ou, encore, dans l'anneau $P[x]$) en un produit de deux*

polynômes de degrés inférieurs à n :

$$f(x) = \varphi(x)\psi(x), \tag{1}$$

et que $f(x)$ est irréductible sur un champ P si toute décomposition de $f(x)$ de la forme (1) contient un facteur de degré nul et un autre facteur de degré n.

Il faut surtout attirer l'attention sur la circonstance que l'on ne peut parler de la réductibilité ou de l'irréductibilité d'un polynôme que par rapport à un champ donné P, car un polynôme irréductible sur P peut être réductible sur une extension $\overline{P}$. Ainsi, le polynôme $x^2 - 2$ à coefficients entiers est irréductible sur le champ des nombres rationnels (il ne peut pas être décomposé en un produit de deux polynômes de degré un à coefficients rationnels). Toutefois, ce même polynôme est réductible sur le champ des nombres réels, comme le prouve l'égalité

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Le polynôme $x^2 + 1$ est non seulement irréductible sur le champ des nombres rationnels, mais aussi sur le champ des nombres réels; néanmoins, il devient réductible sur le champ des nombres complexes, car

$$x^2 + 1 = (x - i)(x + i).$$

Indiquons quelques propriétés fondamentales des polynômes irréductibles, gardant présent à l'esprit qu'il s'agit des polynômes irréductibles sur un *champ* donné P.

α) *Tout polynôme du premier degré est irréductible.*

En effet, si l'on pouvait décomposer un tel polynôme en un produit de deux facteurs de degré inférieur à un, alors les facteurs seraient de degré nul. Or, le produit de polynômes de degré nul est encore un polynôme de degré nul et non du premier degré.

β) *Si un polynôme $p(x)$ est irréductible, alors il en est de même pour tout polynôme $cp(x)$, c étant un élément non nul de P.*

Cette propriété découle des propriétés I et VII du § 21. Elle permettra de nous borner, là où il le faut, à la considération des polynômes irréductibles dont le coefficient du terme principal est l'unité.

γ) *Soient $f(x)$ un polynôme quelconque et $p(x)$ un polynôme irréductible ; alors, $f(x)$ est divisible par $p(x)$, ou $f(x)$ et $p(x)$ sont premiers entre eux.*

Si $(f(x), p(x)) = d(x)$, alors $d(x)$, en tant que diviseur d'un polynôme irréductible $p(x)$, est soit de degré nul, soit de la forme $cp(x)$, $c \neq 0$. Dans le premier cas, $f(x)$ et $p(x)$ sont premiers entre eux, et dans le second $p(x)$ est un diviseur de $f(x)$.

δ) *Si le produit des polynômes $f(x)$ et $g(x)$ est divisible par un polynôme irréductible $p(x)$, alors au moins l'un des facteurs est divisible par $p(x)$.*

En effet, si $f(x)$ n'est pas divisible par $p(x)$, alors, d'après la propriété γ), $f(x)$ et $p(x)$ sont premiers entre eux et, en vertu de b) du § 21, le polynôme $g(x)$ doit avoir $p(x)$ pour diviseur.

La propriété δ) se généralise sans difficulté au cas d'un nombre fini quelconque de facteurs.

La démonstration des deux théorèmes suivants est le but principal de ce paragraphe.

Tout polynôme $f(x)$ de l'anneau $P[x]$ de degré n, $n \geqslant 1$, peut être décomposé en un produit de facteurs irréductibles.

En effet, si le polynôme $f(x)$ est irréductible, alors le produit en question se réduit à un facteur. Si, par contre, $f(x)$ est réductible, alors $f(x)$ peut être décomposé en un produit de facteurs de degrés inférieurs. Si parmi ces facteurs se trouvent des polynômes réductibles, on peut encore les décomposer en facteurs, etc. Le processus s'arrêtera au bout d'un nombre fini de pas, car pour toute décomposition de $f(x)$ en facteurs, la somme des degrés des facteurs est égale à n, de sorte que le nombre de facteurs dépendant de x peut être au plus n.

La décomposition des nombres entiers en facteurs premiers est bien définie, à condition qu'on se borne à la considération des nombres entiers positifs. Dans l'anneau de tous les nombres entiers cette décomposition est unique au signe près: par exemple, $-6 = 2\cdot(-3) = (-2)\cdot 3$, $10 = 2\cdot 5 = (-2)\cdot(-5)$, etc. On retrouve la même situation dans un anneau des polynômes. Soient une décomposition d'un polynôme $f(x)$ en un produit de facteurs irréductibles

$$f(x) = p_1(x)\,p_2(x)\,\ldots\,p_s(x)$$

et des éléments $c_1, c_2, \ldots, c_s$ du champ P tels que leur produit soit égal à l'unité; alors

$$f(x) = [c_1p_1(x)]\cdot[c_2p_2(x)]\,\ldots\,[c_sp_s(x)]$$

est encore, d'après β), une décomposition de $f(x)$ en un produit de facteurs irréductibles. Il se révèle qu'il n'existe pas d'autres décompositions de $f(x)$:

Si un polynôme $f(x)$ de l'anneau $P[x]$ est décomposé de deux manières différentes en facteurs irréductibles

$$f(x) = p_1(x)\,p_2(x)\,\ldots\,p_s(x) = q_1(x)\,q_2(x)\,\ldots\,q_t(x), \tag{2}$$

alors $s = t$ et, les indices étant convenablement choisis, on a les égalités

$$q_i(x) = c_ip_i(x), \qquad i = 1, 2, \ldots, s, \tag{3}$$

c_i étant des éléments non nuls du champ P.

Ce théorème est vrai pour les polynômes du premier degré, ces derniers étant irréductibles. Nous en donnons une démonstration par récurrence sur le degré du polynôme, c'est-à-dire nous démontrons ce théorème pour $f(x)$, en supposant qu'il soit vrai pour tout polynôme de degré inférieur.

$q_1(x)$ étant un diviseur de $f(x)$, on peut affirmer que, en vertu de la propriété δ) et de l'égalité (2), $q_1(x)$ est un diviseur d'au moins d'un des polynômes $p_i(x)$, soit de $p_1(x)$. Le polynôme $p_1(x)$ étant irréductible et $q_1(x)$ de degré non nul, il existe un élément c_1 tel que

$$q_1(x) = c_1 p_1(x). \tag{4}$$

Substituant cette expression de $q_1(x)$ dans (2) et simplifiant (on peut diviser par $p_1(x)$, car l'anneau $P[x]$ n'a pas de diviseurs de zéro), nous obtenons l'égalité

$$p_2(x)\, p_3(x) \ldots p_s(x) = [c_1 q_2(x)]\, q_3(x) \ldots q_t(x).$$

Le degré de ce produit étant inférieur à celui de $f(x)$, on a, d'après l'hypothèse de récurrence, l'égalité: $s - 1 = t - 1$, d'où $s = t$, ainsi que les relations: $c_2' p_2(x) = c_1 q_2(x)$ (ou encore $q_2(x) = (c_1^{-1} c_2')\, p_2(x)$), $c_i p_i(x) = q_i(x)$, $i = 3, \ldots, s$, $c_2', c_3, \ldots, c_s$ étant des éléments non nuls du champ P. Posant $c_1^{-1} c_2' = c_2$ et vu (4), nous obtenons les égalités (3).

Le théorème que nous venons de démontrer peut s'énoncer de manière plus compacte: *tout polynôme se décompose en facteurs irréductibles de façon unique à des facteurs de degré nul près.*

D'ailleurs, on peut se borner à des décompositions de la forme spéciale suivante (*cette décomposition est déjà unique pour tout polynôme*): soit une décomposition quelconque d'un polynôme $f(x)$ en facteurs irréductibles; mettant en facteur le coefficient du terme principal de chaque polynôme irréductible, nous obtenons la décomposition

$$f(x) = a_0 p_1(x)\, p_2(x) \ldots p_s(x), \tag{5}$$

où les polynômes irréductibles $p_i(x)$, $i = 1, 2, \ldots, s$, ont l'unité pour coefficients des termes principaux. En effectuant les multiplications du second membre de (5), il est facile de démontrer que le facteur a_0 n'est autre que le coefficient du terme principal du polynôme $f(x)$.

Les facteurs irréductibles intervenant dans la décomposition (5) ne sont pas forcément tous distincts. Si un polynôme irréductible $p(x)$ est répété k fois dans la décomposition (5), alors $p(x)$ est appelé *facteur multiple* de $f(x)$, plus précisément, d'*ordre de multiplicité* k. Par contre, si un facteur $p(x)$ n'est rencontré qu'une fois dans la décomposition (5), alors $p(x)$ est dit *facteur simple* (ou d'*ordre de multiplicité unité*) de $f(x)$.

Supposons que les facteurs $p_1(x)$, $p_2(x)$, . . ., $p_l(x)$ dans la décomposition (5) soient tous distincts et que tout facteur de $f(x)$ coïncide avec l'un de ces polynômes; supposons, en outre, que $p_i(x)$ soit un facteur d'ordre de multiplicité k_i du polynôme $f(x)$, $i = 1, 2, \ldots, l$, alors la décomposition (5) peut être récrite sous la forme:

$$f(x) = a_0 p_1^{k_1}(x)\, p_2^{k_2}(x) \ldots p_l^{k_l}(x). \qquad (6)$$

C'est précisément cette écriture que nous utiliserons désormais sans mentionner chaque fois que les puissances sont les ordres de multiplicité des facteurs correspondants ou, encore, que $p_i(x) \neq p_j(x)$ pour $i \neq j$.

Soient deux polynômes $f(x)$ et $g(x)$, décomposés chacun en facteurs irréductibles; le plus grand commun diviseur $d(x)$ de $f(x)$ et de $g(x)$ est égal au produit des facteurs intervenant simultanément dans la décomposition de $f(x)$ et de $g(x)$; en outre, tout facteur commun doit être élevé à une puissance égale à l'ordre de multiplicité minimal de ce facteur dans la décomposition de $f(x)$ et de $g(x)$.

En effet, le produit en question est un diviseur de $f(x)$ et de $g(x)$ et, par conséquent, de $d(x)$. Si ce produit était différent de $d(x)$, alors la décomposition de $d(x)$ en facteurs irréductibles contiendrait un facteur n'intervenant pas dans la décomposition d'un des polynômes $f(x)$ et $g(x)$, ce qui est impossible, ou alors l'un des facteurs de $d(x)$ serait de degré supérieur au degré de ce facteur dans la décomposition de $f(x)$ ou de $g(x)$, ce qui est encore impossible.

Ce théorème est analogue à la règle d'après laquelle on cherche le plus grand commun diviseur de nombres entiers. Toutefois, il ne peut pas remplacer l'algorithme d'Euclide dans le cas de polynômes. En effet, puisque les nombres premiers plus petits qu'un nombre entier positif donné forment un ensemble fini, la décomposition d'un nombre entier en facteurs premiers s'obtient après un nombre fini d'essais. Cela n'a pas lieu dans un anneau des polynômes sur un champ de base infini et, dans le cas général, on ne peut pas donner une méthode de décomposition d'un polynôme en facteurs irréductibles. De plus, dire si un polynôme $f(x)$ est irréductible ou réductible sur un champ donné P est déjà, dans le cas général. un problème assez difficile. Ainsi, la description des polynômes irréductibles sur le champ des nombres complexes ou des nombres réels a été obtenue au § 24 comme conséquence du théorème très important sur l'existence d'un zéro. En ce qui concerne le champ des nombres rationnels, nous ne pourrons énoncer au § 56 que quelques résultats de caractère très particulier à ce sujet.

Nous avons montré que dans l'anneau des polynômes, tout comme dans celui des nombres entiers, il existe une décomposition en facteurs « simples » (irréductibles) et que, dans un certain sens, cette décomposition est unique.

On se demande dans quelle mesure on peut étendre ces résultats à des classes plus larges d'anneaux. Nous nous bornons ici à la considération des anneaux commutatifs ayant un élément unité et ne contenant pas de diviseurs de zéro.

On appelle *diviseur de l'unité* tout élément a d'un anneau qui possède un élément inverse a^{-1},

$$aa^{-1}=1.$$

Ce sont les nombres 1 et -1 dans l'anneau des nombres entiers et les polynômes non nuls de degré nul dans l'anneau $P[x]$ qui sont les éléments non nuls du champ P. Un élément c, différent de zéro et qui ne soit pas un diviseur de l'unité, est appelé élément *simple* si dans toute décomposition de c en un produit de deux facteurs, $c=ab$, au moins un des facteurs est diviseur de l'unité. Les éléments simples dans l'anneau des nombres entiers sont les nombres premiers et dans l'anneau des polynômes les polynômes irréductibles.

Peut-on dans un anneau quelconque décomposer tout élément non nul et qui ne soit pas un diviseur de l'unité en un produit de facteurs simples ? Si la réponse est affirmative, cette décomposition serait-elle unique ? L'unicité doit être interprétée de la manière suivante. Soient deux décompositions d'un élément a en facteurs simples

$$a=p_1p_2\ldots p_k=q_1q_2\ldots q_l\,;$$

alors $k=l$, et, les indices étant convenablement choisis, on a

$$q_i=p_ic_i, \qquad i=1, 2, \ldots, k,$$

où c_i est un diviseur de l'unité.

Il s'avère que dans le cas général la réponse aux questions posées est négative. Nous nous bornons à donner un exemple, notamment, *indiquons un anneau où la décomposition en facteurs simples est possible mais n'est pas univoque.*

Considérons les nombres complexes de la forme

$$\alpha=a+b\sqrt{-3}, \tag{7}$$

avec a et b entiers. Ces nombres forment un anneau sans diviseurs de zéro mais avec une unité ; en effet,

$$(a+b\sqrt{-3})(c+d\sqrt{-3})=(ac-3bd)+(bc+ad)\sqrt{-3}. \tag{8}$$

On appelle *norme* d'un nombre $\alpha=a+b\sqrt{-3}$ le nombre entier positif défini par la formule

$$N(\alpha)=a^2+3b^2.$$

D'après (8), *la norme d'un produit est égale au produit des normes,*

$$N(\alpha\beta)=N(\alpha)\,N(\beta). \tag{9}$$

En effet,

$$(ac-3bd)^2+3(bc+ad)^2=a^2c^2+9b^2d^2+3b^2c^2+\\+3a^2d^2=(a^2+3b^2)(c^2+3d^2).$$

Si un nombre α est diviseur de l'unité dans l'anneau considéré, c'est-à-dire si le nombre α^{-1} est encore de la forme (7), alors, d'après (9), on a

$$N(\alpha)\cdot N(\alpha^{-1})=N(\alpha\alpha^{-1})=N(1)=1,$$

de sorte que $N(\alpha)=1$, les nombres $N(\alpha)$ et $N(\alpha^{-1})$ étant entiers positifs. Si $\alpha=a+b\sqrt{-3}$, alors l'égalité $N(\alpha)=1$ entraîne

$$N(\alpha)=a^2+3b^2=1\,;$$

or, cela n'est possible que lorsque $b = 0$, $a = \pm 1$. Ainsi, *l'anneau considéré, tout comme l'anneau des nombres entiers, n'a d'autres diviseurs de l'unité que les nombres 1 et —1 et il n'y a que ces nombres qui aient pour norme l'unité.*

Bien entendu, l'égalité (9) qui exprime la norme d'un produit se généralise au cas d'un nombre fini quelconque de facteurs. Il est facile d'en déduire que *tout nombre α de l'anneau considéré peut être décomposé en un produit d'un nombre fini de facteurs simples*; nous laissons au lecteur le soin de le démontrer.

Mais on ne peut plus affirmer qu'une telle décomposition soit unique. Par exemple, on a les égalités

$$4 = 2\cdot 2 = (1+\sqrt{-3})\,(1-\sqrt{-3}).$$

L'anneau considéré n'ayant pas d'autres diviseurs de l'unité que 1 et —1, le nombre $1+\sqrt{-3}$ (aussi bien que le nombre $1-\sqrt{-3}$) ne peut pas être égal au nombre 2 divisé ou multiplié par un diviseur de l'unité. Il reste à montrer que les nombres $2, 1+\sqrt{-3}, 1-\sqrt{-3}$ sont simples dans l'anneau considéré. En effet, la norme de chacun de ces nombres est égale à 4. Soit α un de ces nombres. Supposons que

$$\alpha = \beta\gamma.$$

Alors, d'après (9), l'un des trois cas suivants est possible:

1) $N(\beta) = 4, \qquad N(\gamma) = 1;$

2) $N(\beta) = 1, \qquad N(\gamma) = 4;$

3) $N(\beta) = N(\gamma) = 2.$

On sait que dans le premier cas le nombre γ est un diviseur de l'unité et que dans le second c'est le nombre β. En ce qui concerne le troisième cas, il ne saurait se réaliser, car il n'existe pas de nombres entiers a et b satisfaisant à l'égalité

$$a^2 + 3b^2 = 2.$$

Facteurs multiples. Bien que nous n'ayons pas de méthode de décomposition d'un polynôme en facteurs irréductibles (on en a déjà parlé ci-dessus), il existe des méthodes permettant de dire si un polynôme donné possède des facteurs multiples et de ramener l'étude d'un polynôme à facteurs multiples à celle d'un polynôme à facteurs simples. Toutefois, ces méthodes imposent certaines restrictions au champ de base. Notamment, dans la suite de ce paragraphe nous supposons que le *champ P soit de caractéristique nulle.* Sans cette restriction les théorèmes sur les facteurs multiples que nous démontrerons ci-dessous ne sont plus valables; en même temps, le cas de champs de caractéristique nulle est, du point de vue des applications, le plus important, car il contient, en particulier, les champs numériques.

Notons d'abord que la notion de *dérivée*, introduite au § 22 pour les polynômes à coefficients complexes, ainsi que les propriétés fondamentales des dérivées se généralisent au cas considéré [1]. Démontrons maintenant le théorème suivant.

[1] La proposition d'après laquelle la dérivée d'un polynôme de degré n est un polynôme de degré $n - 1$ n'est plus vraie pour un champ de caractéristique finie.

Si $p(x)$ est un facteur irréductible d'ordre de multiplicité k d'un polynôme $f(x)$, $k \geqslant 1$, alors $p(x)$ est un facteur d'ordre de multiplicité $k-1$ de la dérivée de $f(x)$. En particulier, un facteur simple d'un polynôme n'intervient pas dans la décomposition de sa dérivée en facteurs irréductibles.

En effet, soit

$$f(x) = p^k(x)\, g(x), \tag{10}$$

où $g(x)$ n'est plus divisible par $p(x)$. Dérivant l'égalité (10), il vient :

$$f'(x) = p^k(x)\, g'(x) + kp^{k-1}(x)\, p'(x)\, g(x) =$$
$$= p^{k-1}(x)\,[p(x)\, g'(x) + kp'(x)\, g(x)].$$

Le second terme entre crochets n'est pas divisible par $p(x)$; en effet, $g(x)$ n'est pas divisible par $p(x)$ en vertu de notre hypothèse, $p'(x)$ est de degré inférieur à celui de $p(x)$, c'est-à-dire qu'il n'est pas divisible par $p(x)$, et il en résulte notre proposition, compte tenu de l'irréductibilité de $p(x)$, de la propriété δ) de ce paragraphe et de IX du § 21. D'autre part, le premier terme de la somme entre crochets est divisible par $p(x)$, de sorte que cette somme ne peut pas être divisible par $p(x)$, c'est-à-dire le facteur $p(x)$ doit, en réalité, intervenir dans l'expression de $f'(x)$ avec l'ordre de multiplicité $k-1$.

De notre théorème et de la méthode de calcul du plus grand commun diviseur de deux polynômes indiquée ci-dessus, il résulte que si la décomposition d'un polynôme $f(x)$ en facteurs irréductibles est de la forme

$$f(x) = a_0 p_1^{k_1}(x)\, p_2^{k_2}(x) \ldots p_l^{k_l}(x), \tag{11}$$

alors *le plus grand commun diviseur du polynôme $f(x)$ et de la dérivée de $f(x)$ admet la décomposition en facteurs irréductibles suivante* :

$$(f(x),\, f'(x)) = p_1^{k_1-1}(x)\, p_2^{k_2-1}(x) \ldots p_l^{k_l-1}(x); \tag{12}$$

bien entendu, ici le facteur $p_i^{k_i-1}(x)$ doit être remplacé par l'unité lorsque $k_i = 1$. En particulier, *le polynôme $f(x)$ ne possède pas de facteurs multiples si et seulement si $f(x)$ et sa dérivée $f'(x)$ sont premiers entre eux.*

Ainsi, nous avons résolu le problème d'existence des facteurs multiples d'un polynôme donné. De plus, vu que la dérivée d'un polynôme et le plus grand commun diviseur de deux polynômes ne dépendent pas de ce que l'on considère un champ de base P ou toute extension de ce champ $\overline{P}$, nous obtenons, comme conséquence du résultat que nous venons de démontrer, la proposition suivante.

Si un polynôme $f(x)$ à coefficients dans un champ P de caractéristique nulle ne possède pas de facteurs multiples sur ce champ, alors il en est de même pour toute extension $\overline{P}$ du champ P.

En particulier, $f(x)$ étant irréductible sur un champ P et $\overline{P}$ étant une extension de P, le polynôme $f(x)$, bien qu'il puisse être réductible sur $\overline{P}$, n'est quand même pas divisible par le carré d'un polynôme irréductible sur $\overline{P}$.

Séparation des facteurs multiples. Soient un polynôme $f(x)$ admettant une décomposition de la forme (11) et le plus grand commun diviseur $d_1(x)$ de $f(x)$ et de sa dérivée; alors (12) est la décomposition de $d_1(x)$. Divisant (11) par (12) il vient

$$v_1(x) = \frac{f(x)}{d_1(x)} = a_0 p_1(x) p_2(x) \ldots p_l(x),$$

c'est-à-dire le quotient est un polynôme sans facteurs multiples; en outre, tout facteur irréductible de $v_1(x)$ est également un facteur de $f(x)$. Cela ramène le problème de calcul des facteurs irréductibles d'un polynôme $f(x)$ au même problème pour le polynôme $v_1(x)$ qui est, en général, de degré inférieur à celui de $f(x)$ et n'a que des facteurs simples. Si nous arrivons à résoudre ce problème pour $v_1(x)$, il ne restera que le problème de la détermination des ordres de multiplicité des facteurs irréductibles de $f(x)$, ce qui peut être fait au moyen de l'algorithme de division.

Appliquant une méthode plus compliquée, basée sur la considération d'un certain nombre de polynômes sans facteurs multiples, nous pouvons non seulement trouver les facteurs irréductibles de $f(x)$, mais aussi les ordres de multiplicité de ces facteurs.

Soit (11) la décomposition de $f(x)$ en facteurs irréductibles; supposons que s, $s \geqslant 1$, soit le plus grand ordre de multiplicité des facteurs de $f(x)$. Notons par $F_1(x)$ le produit des facteurs d'ordre de multiplicité unité du polynôme $f(x)$, chaque facteur étant pris une fois, par $F_2(x)$ le produit des facteurs d'ordre de multiplicité deux, chaque facteur étant pris une fois, etc., enfin, par $F_s(x)$ le produit des facteurs d'ordre de multiplicité s, chaque facteur étant pris une fois. Si le polynôme $f(x)$ n'a pas de facteurs d'ordre de multiplicité j pour un entier j, nous posons alors: $F_j(x) = 1$. Alors $f(x)$ est divisible par la puissance $k^{\text{ème}}$ de $F_k(x)$, $k = 1, 2, \ldots, s$, et la décomposition (11) prend la forme

$$f(x) = a_0 F_1(x) F_2^2(x) F_3^3(x) \ldots F_s^s(x),$$

tandis que la décomposition (12) de $d_1(x) = (f(x), f'(x))$ peut être récrite de façon suivante:

$$d_1(x) = F_2(x) F_3^2(x) \ldots F_s^{s-1}(x).$$

Notant par $d_2(x)$ le plus grand commun diviseur du polynôme $d_1(x)$ et de la dérivée $d_1'(x)$ et, plus généralement, par $d_k(x)$ le plus grand commun divi-

seur des polynômes $d_{k-1}(x)$ et $d'_{k-1}(x)$, nous obtenons de la même manière:

$$d_2(x) = F_3(x) F_4^2(x) \dots F_s^{s-2}(x),$$

$$d_3(x) = F_4(x) F_5^2(x) \dots F_s^{s-3}(x),$$

$$\dots\dots\dots\dots$$

$$d_{s-1}(x) = F_s(x),$$

$$d_s(x) = 1.$$

On en déduit

$$v_1(x) = \frac{f(x)}{d_1(x)} = a_0 F_1(x) F_2(x) F_3(x) \dots F_s(x),$$

$$v_2(x) = \frac{d_1(x)}{d_2(x)} = F_2(x) F_3(x) \dots F_s(x),$$

$$v_3(x) = \frac{d_2(x)}{d_3(x)} = F_3(x) \dots F_s(x),$$

$$\dots\dots\dots\dots$$

$$v_s(x) = \frac{d_{s-1}(x)}{d_s(x)} = F_s(x),$$

et, par conséquent, on a finalement

$$F_1(x) = \frac{v_1(x)}{a_0 v_2(x)}, \quad F_2(x) = \frac{v_2(x)}{v_3(x)}, \quad \dots, \quad F_s(x) = v_s(x).$$

Ainsi, n'utilisant que des procédés qui ne supposent pas la connaissance des facteurs irréductibles de $f(x)$, notamment, n'utilisant que la dérivation, l'algorithme d'Euclide et l'algorithme de division, nous pouvons calculer les polynômes $F_1(x)$, $F_2(x)$, $\dots$, $F_s(x)$ qui n'ont pas de facteurs multiples; en outre, tout facteur irréductible du polynôme $F_k(x)$, $k = 1, 2, \dots, s$, est un facteur d'ordre de multiplicité k de $f(x)$.

Evidemment, la méthode exposée ci-dessus ne saurait pas être considérée comme une méthode de décomposition d'un polynôme en facteurs irréductibles, car dans le cas où $s = 1$, c'est-à-dire pour les polynômes sans facteurs multiples, cette méthode ne donne que $f(x) = F_1(x)$.

§ 49*. Théorème d'existence d'un zéro

Bien entendu, le théorème fondamental sur l'existence d'un zéro de tout polynôme d'une indéterminée numérique sur le champ des nombres complexes, démontré au § 23, ne peut pas être étendu au cas d'un champ quelconque. Nous démontrerons dans ce paragraphe un théorème qui, dans un certain sens, occupe la même place dans la théorie générale des champs algébriques que le théorème fondamental de l'algèbre des nombres complexes.

Soit un polynôme $f(x)$ sur un champ P. Il est naturel de poser le problème suivant: le polynôme $f(x)$ n'ayant pas de zéros dans le champ P, existe-t-il une extension $\overline{P}$ du champ P telle que $f(x)$ possède au moins un zéro dans $\overline{P}$? Ici on peut supposer que le degré

du polynôme $f(x)$ est supérieur à l'unité, car pour les polynômes de degré nul le problème n'a pas de sens et tout polynôme du premier degré, soit $ax+b$, possède le zéro $-\frac{b}{a}$ dans le champ P lui-même. D'autre part, on peut, évidemment, se limiter au cas où $f(x)$ est irréductible: si $f(x)$ est réductible sur le champ P, alors un zéro de tout facteur irréductible est, en même temps, un zéro de $f(x)$.

La solution du problème qui nous intéresse est donnée par le *théorème* suivant *sur l'existence d'un zéro*:

Pour tout polynôme $f(x)$ irréductible sur un champ P il existe une extension de P telle qu'elle contienne au moins un zéro de $f(x)$. Tous les champs minimaux contenant le champ P et un zéro du polynôme sont isomorphes.

Démontrons d'abord la seconde partie du théorème.

Soit un polynôme irréductible sur un champ P

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n, \tag{1}$$

où $n \geqslant 2$, c'est-à-dire on suppose que $f(x)$ n'ait pas de zéros dans le champ P. Supposons qu'il existe une extension $\overline{P}$ du champ P contenant un zéro, soit α, de $f(x)$; démontrons le lemme suivant, nécessaire pour la suite et présentant un intérêt par lui-même:

Soit α un zéro dans $\overline{P}$ d'un polynôme $f(x)$ irréductible sur P; supposons que α soit également un zéro d'un polynôme $g(x)$ de l'anneau $P[x]$. Alors $f(x)$ est un diviseur de $g(x)$.

En effet, considérés sur le champ $\overline{P}$, les polynômes $f(x)$ et $g(x)$ possèdent un diviseur commun $x-\alpha$ et, par conséquent, ne sont pas premiers entre eux. La propriété des polynômes de ne pas être premiers entre eux ne dépend pas du choix d'un champ, de sorte que nous pouvons passer au champ P et appliquer la propriété γ) du paragraphe précédent.

Trouvons maintenant le sous-champ minimal $P(\alpha)$ du champ $\overline{P}$, contenant le champ P et l'élément α. $P(\alpha)$ contient, en tout cas, les éléments de la forme

$$\beta=b_0+b_1\alpha+b_2\alpha^2+\ldots+b_{n-1}\alpha^{n-1}, \tag{2}$$

où $b_0, b_1, b_2, \ldots, b_{n-1}$ sont des éléments du champ P. Il n'existe pas d'éléments du champ $\overline{P}$ ayant deux écritures différentes (2); en effet, si on a, en même temps,

$$\beta=c_0+c_1\alpha+c_2\alpha^2+\ldots+c_{n-1}\alpha^{n-1},$$

et $c_k \neq b_k$ au moins pour un k, alors α est un zéro du polynôme

$$g(x)=(b_0-c_0)+(b_1-c_1)x+(b_2-c_2)x^2+\ldots+(b_{n-1}-c_{n-1})x^{n-1},$$

ce qui est en contradiction avec le lemme démontré ci-dessus, vu que le degré de $g(x)$ est inférieur à celui de $f(x)$.

L'ensemble des éléments du champ $\overline{P}$ de la forme (2) contient les éléments du champ P ($b_1 = b_2 = \ldots = b_{n-1} = 0$) et l'élément α ($b_1 = 1$, $b_0 = b_2 = \ldots = b_{n-1} = 0$). Montrons que les *éléments de la forme* (2) *constituent le sous-champ cherché* $P(\alpha)$. En effet, soient un élément β (écrit sous la forme (2)) et un élément γ,

$$\gamma = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1};$$

les propriétés des opérations sur le champ $\overline{P}$ donnent

$$\beta \pm \gamma = (b_0 \pm c_0) + (b_1 \pm c_1)\,\alpha + (b_2 \pm c_2)\,\alpha^2 + \ldots + (b_{n-1} \pm c_{n-1})\,\alpha^{n-1},$$

c'est-à-dire la somme et la différence de tout couple d'éléments de la forme (2) sont encore des éléments de cette forme.

Multipliant β et γ nous obtenons une expression contenant α^n et des puissances de α d'exposants supérieurs à n. Néanmoins, de la formule (1) et de l'égalité $f(\alpha) = 0$ il découle que α^n et, par conséquent, α^{n+1}, α^{n+2}, etc. peuvent être exprimés par des puissances de α d'exposants inférieurs à n. La plus simple méthode de trouver l'expression de $\beta\gamma$ est la suivante: posons

$$\varphi(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1},$$
$$\psi(x) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1},$$

de sorte que $\varphi(\alpha) = \beta$, $\psi(\alpha) = \gamma$. Multipliant les polynômes $\varphi(x)$ et $\psi(x)$ et divisant avec reste le produit par $f(x)$, il vient

$$\varphi(x)\,\psi(x) = f(x)\,q(x) + r(x), \tag{3}$$

avec

$$r(x) = d_0 + d_1x + \ldots + d_{n-1}x^{n-1}.$$

Faisant $x = \alpha$ dans les deux membres de l'égalité (3), nous obtenons

$$\varphi(\alpha)\,\psi(\alpha) = f(\alpha)\,q(\alpha) + r(\alpha),$$

ou encore, vu que $f(\alpha) = 0$,

$$\beta\gamma = d_0 + d_1\alpha + \ldots + d_{n-1}\alpha^{n-1}.$$

Ainsi, le produit de deux éléments de la forme (2) est encore un élément de la forme (2).

Enfin, montrons que si un élément β est de la forme (2) et $\beta \neq 0$, alors l'élément β^{-1}, qui existe dans le champ $\overline{P}$, peut être également mis sous la forme (2). Pour cela fixons dans l'anneau $P[x]$ un polynôme

$$\varphi(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}.$$

Le degré de $\varphi(x)$ étant inférieur à celui de $f(x)$ et le polynôme $f(x)$ étant irréductible sur le champ P, les polynômes $\varphi(x)$ et $f(x)$

sont premiers entre eux, de sorte que, d'après les §§ 21 et 47, il existe dans l'anneau $P[x]$ des polynômes $u(x)$ et $v(x)$ tels que l'on ait

$$\varphi(x)u(x)+f(x)v(x)=1;$$

en outre, on peut supposer que le degré de $u(x)$ est inférieur à n:

$$u(x)=s_0+s_1x+\ldots+s_{n-1}x^{n-1}.$$

Il en résulte, vu l'égalité $f(\alpha)=0$, que

$$\varphi(\alpha)u(\alpha)=1,$$

de sorte que, vu l'égalité $\varphi(\alpha)=\beta$, nous obtenons

$$\beta^{-1}=u(\alpha)=s_0+s_1\alpha+\ldots+s_{n-1}\alpha^{n-1}.$$

Ainsi, l'ensemble des éléments de la forme (2) est un sous-champ du champ $\overline{P}$; cet ensemble est le champ cherché $P(\alpha)$. Ensuite, on a vu que pour trouver la somme et le produit de deux éléments β et γ de la forme (2), il suffit de connaître les coefficients dans leurs expressions suivant les puissances de α; on peut, donc, affirmer que le résultat suivant est vrai: supposons que, outre $\overline{P}$, il existe une autre extension $\overline{P}'$ du champ P, $\overline{P}'$ contenant aussi un zéro α' du polynôme $f(x)$; soit $P(\alpha')$ un sous-champ minimal du champ $\overline{P}'$, contenant P et α', alors les *champs* $P(\alpha)$ et $P(\alpha')$ *sont isomorphes*; en outre, l'isomorphisme des champs $P(\alpha)$ et $P(\alpha')$ s'obtient en faisant correspondre à tout élément de $P(\alpha)$ de la forme (2) l'élément de $P(\alpha')$ ayant les mêmes coefficients .

$$\beta'=b_0+b_1\alpha'+b_2\alpha'^2+\ldots+b_{n-1}\alpha'^{n-1}.$$

Ceci démontre la seconde partie du théorème.

Passons à la démonstration de la première partie du théorème; en outre, ce qui a été exposé ci-dessus nous suggérera la voie de démonstration. Nous avons un polynôme $f(x)$ de degré n, $n \geqslant 2$, irréductible sur un champ P; il s'agit de construire une extension du champ P, contenant un zéro de $f(x)$. A ce dessein représentons l'anneau des polynômes $P[x]$ comme réunion de classes disjointes de polynômes, chaque classe se composant de polynômes ayant le même reste de division par $f(x)$. Autrement dit, deux polynômes $\varphi(x)$ et $\psi(x)$ appartiennent à une même classe si leur différence est divisible par $f(x)$.

Convenons de noter les classes obtenues par les lettres A, B, C, etc., et définissons de façon naturelle la somme et le produit de classes. Notamment, soient deux classes A et B, un polynôme $\varphi_1(x)$ de la classe A et un polynôme $\psi_1(x)$ de la classe B; désignons

par $\chi_1(x)$ la somme des polynômes $\varphi_1(x)$ et $\psi_1(x)$,

$$\chi_1(x) = \varphi_1(x) + \psi_1(x),$$

et par $\theta_1(x)$ leur produit,

$$\theta_1(x) = \varphi_1(x) \cdot \psi_1(x).$$

Choisissons maintenant dans la classe A un autre polynôme $\varphi_2(x)$ et dans la classe B un polynôme $\psi_2(x)$; désignons par $\chi_2(x)$ et $\theta_2(x)$ respectivement leur somme et leur produit:

$$\chi_2(x) = \varphi_2(x) + \psi_2(x),$$
$$\theta_2(x) = \varphi_2(x) \cdot \psi_2(x).$$

Les polynômes $\varphi_1(x)$ et $\varphi_2(x)$ appartenant tous les deux à la classe A, leur différence $\varphi_1(x) - \varphi_2(x)$ est divisible par $f(x)$; la différence $\psi_1(x) - \psi_2(x)$ jouit de la même propriété. Il en résulte que la différence

$$\chi_1(x) - \chi_2(x) = [\varphi_1(x) + \psi_1(x)] - [\varphi_2(x) + \psi_2(x)] = \\ = [\varphi_1(x) - \varphi_2(x)] + [\psi_1(x) - \psi_2(x)] \qquad (4)$$

est encore divisible par $f(x)$. La même chose est vraie pour $\theta_1(x) - \theta_2(x)$, car

$$\theta_1(x) - \theta_2(x) = \varphi_1(x)\psi_1(x) - \varphi_2(x)\psi_2(x) = \\ = \varphi_1(x)\psi_1(x) - \varphi_1(x)\psi_2(x) + \varphi_1(x)\psi_2(x) - \varphi_2(x)\psi_2(x) = \\ = \varphi_1(x)[\psi_1(x) - \psi_2(x)] + [\varphi_1(x) - \varphi_2(x)]\psi_2(x). \qquad (5)$$

L'égalité (4) montre que les polynômes $\chi_1(x)$ et $\chi_2(x)$ appartiennent à une même classe. Autrement dit, la somme d'un polynôme de la classe A et d'un polynôme de la classe B appartient à une classe bien définie C qui ne dépend pas du choix des polynômes qu'on fixe pour « représenter » respectivement la classe A et la classe B ; appelons la classe C *somme* des classes A et B :

$$C = A + B.$$

De même, vu l'égalité (5), la classe D, contenant le produit d'un polynôme de A et d'un polynôme de B, ne dépend pas du choix des polynômes représentant les classes A et B ; nous appelons la classe D *produit* des classes A et B :

$$D = AB.$$

Montrons que l'ensemble des classes (dont la réunion donne l'anneau $P[x]$), pourvu des opérations d'addition et de multiplication définies ci-dessus, devient un champ. En effet, l'*associativité* et la *commutativité* des deux opérations, ainsi que la *distributivité*,

découlent des propriétés correspondantes des opérations sur l'anneau $P[x]$, car les opérations sur les classes se ramènent aux mêmes opérations sur les polynômes appartenant à ces classes. L'élément *nul* est manifestement la classe composée des polynômes divisibles par le polynôme $f(x)$. Cette classe, notée par le symbole 0, est appelée *classe nulle*. La classe *opposée* à une classe A (la classe A étant composée des polynômes divisibles avec le reste $\varphi(x)$ par $f(x)$) est composée des polynômes qui, divisés par $f(x)$, donnent pour reste $-\varphi(x)$. Il en résulte l'existence de l'opération de *soustraction* bien définie dans l'ensemble des classes.

Afin de démontrer qu'il existe une *division* dans l'ensemble des classes, il faut montrer, d'une part, l'existence d'une classe tenant le rôle de l'unité et, d'autre part, l'existence de la classe inverse pour toute classe non nulle. Il est clair que le rôle de l'*unité* est tenu par les polynômes qui, divisés par $f(x)$, donnent l'unité pour reste; la classe de ces polynômes, appelée *classe unité*, est notée par le symbole E.

Soit maintenant une classe non nulle A. Par conséquent, tout polynôme $\varphi(x)$, représentant de la classe A, divisé par $f(x)$, donne un reste non nul, de sorte que, vu l'irréductibilité de $f(x)$, les polynômes $\varphi(x)$ et $f(x)$ sont premiers entre eux. Il existe, donc, dans l'anneau $P[x]$ deux polynômes $u(x)$ et $v(x)$ satisfaisant à l'égalité

$$\varphi(x)u(x)+f(x)v(x)=1,$$

ou, encore, à l'égalité

$$\varphi(x)u(x)=1-f(x)v(x). \tag{6}$$

Le second membre de (6), divisé par $f(x)$, donne l'unité pour reste, c'est-à-dire il appartient à la classe unité E. Notant par B la classe contenant le polynôme $u(x)$, l'égalité (6) prend la forme

$$AB=E,$$

d'où l'on a $B=A^{-1}$. Ceci démontre l'existence d'une classe inverse pour toute classe non nulle, autrement dit, on a montré que les classes forment un champ.

Désignons ce champ par $\overline{P}$ et montrons que *$\overline{P}$ est une extension du champ P*. A tout élément a du champ P correspond une classe composée de polynômes qui, divisés par $f(x)$, donnent a pour reste; l'élément a, en tant que polynôme de degré nul, appartient à cette classe. Les classes de cette forme spéciale forment dans $\overline{P}$ un sous-champ isomorphe au champ P. En effet, l'application bijective est claire; d'autre part, choisissant comme représentants des classes considérées les éléments du champ P, la somme (le produit) d'éléments de P correspond à la somme (au produit) de classes. Ainsi,

par la suite, nous aurons le droit de ne faire aucune distinction entre les éléments du champ P et les classes correspondantes.

Enfin, désignons par X la classe composée de polynômes divisibles par $f(x)$ avec le reste x. Cette classe est un élément bien défini du champ $\overline{P}$; nous voulons montrer que *cet élément est zéro du polynôme* $f(x)$. Soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Notons par A_i la classe qui correspond (dans le sens indiqué ci-dessus) à l'élément a_i du champ P, $i = 0, 1, \ldots, n$; déterminons l'élément du champ $\overline{P}$ qui est de la forme

$$A_0X^n + A_1X^{n-1} + \ldots + A_{n-1}X + A_n. \tag{7}$$

Choisissant comme représentants des classes A_i les éléments a_i, $i = 0, 1, \ldots, n$, et comme représentant de la classe X l'élément x, nous constatons, tenant compte de la définition des opérations d'addition et de multiplication de classes, que la classe (7) contient le polynôme $f(x)$. Or, le polynôme $f(x)$ est divisible par lui-même, de sorte que la classe (7) est la classe nulle. Ainsi, remplaçant dans (7) les classes A_i par les éléments correspondants a_i du champ P, nous obtenons dans le champ $\overline{P}$ l'égalité

$$a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n = 0,$$

c'est-à-dire la classe X est réellement un zéro du polynôme $f(x)$.

Ceci achève la démonstration du théorème d'existence d'un zéro. Notons que *si P est le champ des nombres réels et $f(x) = x^2 + 1$, alors nous obtenons encore un moyen de construction du champ des nombres complexes.*

On peut déduire du théorème d'existence d'un zéro des conséquences analogues à celles du théorème fondamental de l'algèbre des nombres complexes du § 24. Faisons d'abord une remarque.

Tout facteur linéaire $x - c$ d'un polynôme $f(x)$ étant irréductible, le polynôme $x - c$ doit intervenir dans la décomposition *bien définie* de $f(x)$ en facteurs irréductibles.

Toutefois, le nombre de facteurs linéaires dans la décomposition de $f(x)$ en facteurs irréductibles ne peut être supérieur au degré de $f(x)$. Nous sommes, donc, conduits au résultat suivant:

Un polynôme $f(x)$ de degré n ne peut pas avoir dans un champ P plus de n zéros, même si tout zéro est pris avec son ordre de multiplicité.

On appelle *champ de décomposition* d'un polynôme $f(x)$ de degré n sur un champ P une extension Q du champ P telle que $f(x)$ ait exactement n zéros dans le champ Q, tout zéro devant être pris avec son ordre de multiplicité. Le polynôme $f(x)$ sur le champ Q se décom-

pose, donc, en un produit de facteurs linéaires; de plus, aucune extension du champ Q ne peut faire apparaître de nouveaux zéros de $f(x)$.

Il existe pour tout polynôme $f(x)$ de l'anneau $P[x]$ sur un champ P un champ de décomposition.

En effet, si un polynôme $f(x)$ de degré n, $n \geqslant 1$, possède n zéros dans le champ P, alors P est le champ de décomposition en question. Si, par contre, $f(x)$ ne peut pas être décomposé sur le champ P en un produit de facteurs linéaires, alors fixant un des facteurs irréductibles de $f(x)$ de degré supérieur au premier, soit $\varphi(x)$, nous pouvons, en vertu du théorème d'existence d'un zéro, trouver une extension du champ P, soit P', telle que P' contienne un zéro de $\varphi(x)$. Si le polynôme $f(x)$ considéré sur le champ P' ne se décompose pas toujours en un produit de facteurs linéaires, alors construisons encore une extension du champ P', qui contiendrait un zéro d'un des facteurs irréductibles de degré supérieur au premier intervenant dans la décomposition de $f(x)$. Après un nombre fini de pas nous arrivons évidemment à un champ de décomposition de $f(x)$.

Il est clair qu'un polynôme $f(x)$ sur un champ P peut avoir une multitude de champs de décomposition. On pourrait démontrer que les champs minimaux contenant le champ P et n zéros du polynôme $f(x)$ (n étant le degré de $f(x)$) sont tous isomorphes. Mais nous n'utilisons pas cette proposition et, pour cette raison, nous ne donnons pas sa démonstration.

Zéros multiples. Nous avons démontré dans le paragraphe précédent qu'un polynôme $f(x)$ sur un champ P de caractéristique nulle ne possédait pas de facteurs multiples si et seulement si $f(x)$ et la dérivée $f'(x)$ étaient des polynômes premiers entre eux. Nous avons également remarqué que l'absence de facteurs multiples pour un polynôme $f(x)$ sur un champ P garantissait l'absence de facteurs multiples de $f(x)$ sur toute extension $\overline{P}$ de P. Appliquant ce résultat au cas d'un champ de décomposition $\overline{P}$ de $f(x)$ et rappelant la définition de zéros multiples, nous avons la proposition suivante:

Si un polynôme $f(x)$ sur un champ P de caractéristique nulle ne possède pas de zéros multiples dans un champ de décomposition donné, alors $f(x)$ et sa dérivée $f'(x)$ sont premiers entre eux. Réciproquement, si $f(x)$ et sa dérivée $f'(x)$ sont premiers entre eux, alors le polynôme $f(x)$ ne possède de zéros multiples dans aucun champ de décomposition.

Il en résulte, en particulier, qu'un *polynôme $f(x)$ irréductible sur un champ P de caractéristique nulle ne peut avoir de zéros multiples dans aucune extension du champ P.* Dans le cas de champs de caractéristique finie cette proposition cesse d'être vraie, circonstance tenant un rôle important dans la théorie générale des champs algébriques.

Notons pour conclure que les *formules de Viète* (cf. § 24) *sont conservées dans un champ quelconque*; en outre, les zéros du polynôme appartiennent à un champ de décomposition de ce polynôme.

§ 50*. Champ des fractions rationnelles

La théorie des fractions rationnelles, exposée au § 25, *se généralise au cas d'un champ de base quelconque.* Mais, en passant du champ des nombres réels à un champ quelconque P, nous devons renoncer à considérer l'expression $\frac{f(x)}{g(x)}$ comme une *fonction* de la variable x, car ce point de vue n'est plus applicable même dans le cas des polynômes. On se propose d'attribuer un sens à une telle expression lorsque les coefficients appartiennent à un champ quelconque P. Plus précisément, nous voulons construire un champ qui contiendrait l'anneau des polynômes $P[x]$ et tel que les opérations d'addition et de multiplication, définies sur ce champ, coïncident dans le cas des polynômes avec celles sur l'anneau $P[x]$; bref, l'anneau $P[x]$ doit être un *sous-anneau* du champ en question. D'autre part, tout élément du champ cherché doit se représenter comme quotient de deux polynômes (le quotient devant être interprété du point de vue de la division définie sur ce champ). Nous allons montrer que pour tout P on peut construire un tel champ; il est noté $P(x)$ (l'indéterminée est encadrée par des parenthèses et non par des crochets!) et dit *champ des fractions rationnelles* sur un champ P.

Supposons d'abord que l'anneau $P[x]$ soit un sous-anneau d'un champ Q. Soient $f(x)$ et $g(x)$ deux polynômes de $P[x]$; en outre, $g(x) \neq 0$. Alors il existe dans le champ Q un élément, bien défini, égal au quotient de la division de $f(x)$ par $g(x)$. Notant cet élément par $\frac{f(x)}{g(x)}$, comme il est admis de le faire dans le cas d'un champ, nous pouvons écrire, utilisant la définition d'un quotient:

$$f(x) = g(x) \cdot \frac{f(x)}{g(x)}, \tag{1}$$

le produit devant être interprété du point de vue de la multiplication dans le champ Q. Il peut arriver que deux quotients, soit $\frac{f(x)}{g(x)}$ et $\frac{\varphi(x)}{\psi(x)}$, définissent un même élément du champ Q; ceci a lieu si nous avons la condition ordinaire d'égalité de deux fractions:

On a $\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)}$ *si et seulement si* $f(x)\psi(x) = \varphi(x)g(x)$.

En effet, si $\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)} = \alpha$, alors, d'après (1), on a

$$f(x) = g(x)\alpha, \quad \varphi(x) = \psi(x)\alpha,$$

d'où

$$f(x)\,\psi(x)=g(x)\,\psi(x)\,\alpha=g(x)\,\varphi(x).$$

Inversement, si $f(x)\psi(x)=g(x)\varphi(x)=u(x)$ dans le sens de la multiplication dans $P[x]$, alors passant au champ Q, on obtient les égalités :

$$\frac{f(x)}{g(x)}=\frac{u(x)}{g(x)\,\psi(x)}=\frac{\varphi(x)}{\psi(x)}.$$

Ensuite, il est facile de voir que la somme et le produit de deux éléments de Q, qui sont quotients de polynômes de $P[x]$, sont encore des quotients de polynômes de $P[x]$; en outre, les règles ordinaires d'addition et de multiplication de fractions sont valables:

$$\frac{f(x)}{g(x)}+\frac{\varphi(x)}{\psi(x)}=\frac{f(x)\,\psi(x)+g(x)\,\varphi(x)}{g(x)\,\psi(x)}, \tag{2}$$

$$\frac{f(x)}{g(x)}\cdot\frac{\varphi(x)}{\psi(x)}=\frac{f(x)\cdot\varphi(x)}{g(x)\cdot\psi(x)}. \tag{3}$$

En effet, multipliant les deux membres des égalités (2) et (3) par le produit $g(x)\psi(x)$ et appliquant (1) nous obtenons des égalités vraies dans l'anneau $P[x]$. A présent, les égalités (2) et (3) découlent du fait que, vu l'absence de diviseurs du zéro dans Q, les deux membres de chaque égalité obtenue de cette manière peuvent être simplifiés par un élément non nul $g(x)\psi(x)$ en conservant les égalités.

Ces préliminaires suggèrent une voie de construction du champ $P(x)$. Soient un champ P et l'anneau des polynômes $P[x]$ sur le champ P. Faisons correspondre à tout couple ordonné de polynômes $f(x)$ et $g(x)$ de $P[x]$, avec $g(x)\neq 0$, un symbole $\frac{f(x)}{g(x)}$ appelé *fraction rationnelle de numérateur $f(x)$ et de dénominateur $g(x)$*. Soulignons que ce n'est qu'un symbole, car la division dans l'anneau $P[x]$ est, dans le cas général, impossible et l'anneau $P[x]$, pour le moment, n'appartient à aucun champ; quand bien même $g(x)$ serait un diviseur de $f(x)$, il ne faut pas encore confondre le polynôme, quotient de la division de $f(x)$ par $g(x)$, et le symbole $\frac{f(x)}{g(x)}$.

Maintenant, deux fractions rationnelles $\frac{f(x)}{g(x)}$ et $\frac{\varphi(x)}{\psi(x)}$ sont dites *égales* et on écrit :

$$\frac{f(x)}{g(x)}=\frac{\varphi(x)}{\psi(x)}, \tag{4}$$

si on a dans l'anneau $P[x]$ l'égalité $f(x)\psi(x)=g(x)\varphi(x)$. Il est clair que toute fraction est égale à elle-même et que si une fraction est égale à une autre, alors cette dernière est égale à la première. Montrons la *transitivité* de cette notion d'égalité. Soient l'égalité (4)

et l'égalité

$$\frac{\varphi(x)}{\psi(x)} = \frac{u(x)}{v(x)}. \tag{5}$$

Les égalités

$$f(x)\psi(x) = g(x)\varphi(x), \quad \varphi(x)v(x) = \psi(x)u(x),$$

équivalentes à (4) et (5) dans l'anneau $P[x]$, entraînent :

$$f(x)v(x)\psi(x) = g(x)\varphi(x)v(x) = g(x)u(x)\psi(x);$$

donc, simplifiant par l'élément non nul qu'est le polynôme $\psi(x)$ ($\psi(x)$ est non nul en tant que dénominateur d'une des fractions), il vient

$$f(x)v(x) = g(x)u(x),$$

d'où, en vertu de la définition de l'égalité des fractions, on a

$$\frac{f(x)}{g(x)} = \frac{u(x)}{v(x)},$$

ce qu'il fallait démontrer.

Réunissons maintenant en une classe toutes les fractions égales à une même fraction; en vertu de la transitivité de l'égalité, les fractions d'une même classe sont égales. Si une classe contient une fraction qui n'appartient pas à une autre classe, alors ces deux classes n'ont pas d'éléments communs, comme il s'ensuit de la transitivité de l'égalité.

Ainsi, l'ensemble des fractions rationnelles, écrites au moyen des polynômes de l'anneau $P[x]$, est une réunion de classes disjointes, chaque classe étant composée des fractions égales. A présent, nous voulons définir les opérations algébriques sur l'*ensemble de ces classes* de manière qu'il devienne un champ. Définissant les opérations sur les fractions rationnelles, nous devons vérifier chaque fois qu'en remplacant les termes (les facteurs) par des fractions égales, la somme (le produit) se trouve remplacée par une fraction égale. Cela nous autorisera à parler d'une somme et d'un produit, bien définis, des classes de fractions égales.

Faisons d'abord une remarque qui, par la suite, sera utilisée plus d'une fois: *multipliant le numérateur et le dénominateur d'une fraction rationnelle par un même polynôme non nul ou les simplifiant par un diviseur commun, nous obtenons une fraction rationnelle égale à celle donnée initialement.* En effet,

$$\frac{f(x)}{g(x)} = \frac{f(x)h(x)}{g(x)h(x)},$$

car on a dans l'anneau $P[x]$:

$$f(x)[g(x)h(x)] = g(x)[f(x)h(x)].$$

Définissons l'*addition* des fractions rationnelles par la formule (2); vu que $g(x) \neq 0$ et $\psi(x) \neq 0$, on a: $g(x)\psi(x) \neq 0$, de sorte que le second membre dans (2) est, en effet, une fraction rationnelle. Puis, soient

$$\frac{f(x)}{g(x)} = \frac{f_0(x)}{g_0(x)}, \quad \frac{\varphi(x)}{\psi(x)} = \frac{\varphi_0(x)}{\psi_0(x)},$$

ou, encore,

$$f(x)\,g_0(x) = g(x)\,f_0(x), \quad \varphi(x)\,\psi_0(x) = \psi(x)\,\varphi_0(x); \tag{6}$$

multipliant les deux membres de la première égalité (6) par $\psi(x)\,\psi_0(x)$ et la seconde par $g(x)\,g_0(x)$ et additionnant les égalités obtenues, il vient:

$$[f(x)\,\psi(x) + g(x)\,\varphi(x)]\,g_0(x)\,\psi_0(x) =$$
$$= [f_0(x)\,\psi_0(x) + g_0(x)\,\varphi_0(x)]\,g(x)\,\psi(x),$$

ce qui est équivalent à l'égalité

$$\frac{f(x)\,\psi(x) + g(x)\,\varphi(x)}{g(x)\,\psi(x)} = \frac{f_0(x)\,\psi_0(x) + g_0(x)\,\varphi_0(x)}{g_0(x)\,\psi_0(x)}.$$

Ainsi, soient deux classes de fractions égales; alors la somme de toute fraction de la première classe et de toute fraction de la seconde donne une même fraction, c'est-à-dire qu'elle appartient à une troisième classe bien définie. Cette classe est la *somme* des classes données.

La *commutativité* de l'addition ainsi définie résulte directement de la formule (2), tandis que l'*associativité* se démontre de manière suivante:

$$\left[\frac{f(x)}{g(x)} + \frac{\varphi(x)}{\psi(x)}\right] + \frac{u(x)}{v(x)} = \frac{f(x)\,\psi(x) + g(x)\,\varphi(x)}{g(x)\,\psi(x)} + \frac{u(x)}{v(x)} =$$
$$= \frac{f(x)\,\psi(x)\,v(x) + g(x)\,\varphi(x)\,v(x) + g(x)\,\psi(x)\,u(x)}{g(x)\,\psi(x)\,v(x)} =$$
$$= \frac{f(x)}{g(x)} + \frac{\varphi(x)\,v(x) + \psi(x)\,u(x)}{\psi(x)\,v(x)} = \frac{f(x)}{g(x)} + \left[\frac{\varphi(x)}{\psi(x)} + \frac{u(x)}{v(x)}\right].$$

Il découle aisément de la définition de l'égalité de deux fractions que les fractions de la forme $\frac{0}{g(x)}$, c'est-à-dire les fractions à numérateur nul, sont toutes égales et forment une classe complète de fractions égales. Appelons cette classe la classe *nulle* et montrons qu'elle tient le rôle de l'élément nul par rapport à l'addition définie ci-dessus. En effet, soit une fraction $\frac{\varphi(x)}{\psi(x)}$; alors

$$\frac{0}{g(x)} + \frac{\varphi(x)}{\psi(x)} = \frac{0 \cdot \psi(x) + g(x)\,\varphi(x)}{g(x)\,\psi(x)} = \frac{g(x)\,\varphi(x)}{g\psi(x)\;(x)} = \frac{\varphi(x)}{\psi(x)}.$$

De l'égalité

$$\frac{f(x)}{g(x)} + \frac{-f(x)}{g(x)} = \frac{0}{g^2(x)},$$

dont le second membre appartient à la classe nulle, il s'ensuit que la classe des fractions de la forme $\frac{-f(x)}{g(x)}$ est une classe *opposée* à celle contenant les fractions égales à $\frac{f(x)}{g(x)}$. On sait déjà qu'il en résulte l'existence de la *soustraction* bien définie.

Définissons la *multiplication* des fractions rationnelles par la formule (3); en outre, vu que $g(x)\,\psi(x) \neq 0$, le second membre dans (3) est, réellement, une fraction rationnelle. Soient ensuite

$$\frac{f(x)}{g(x)} = \frac{f_0(x)}{g_0(x)}, \quad \frac{\varphi(x)}{\psi(x)} = \frac{\varphi_0(x)}{\psi_0(x)},$$

c'est-à-dire soient

$$f(x)\,g_0(x) = g(x)\,f_0(x), \quad \varphi(x)\,\psi_0(x) = \psi(x)\,\varphi_0(x);$$

multipliant les deux dernières égalités, il vient

$$f(x)\,g_0(x)\,\varphi(x)\,\psi_0(x) = g(x)\,f_0(x)\,\psi(x)\,\varphi_0(x),$$

ce qui est équivalent à l'égalité

$$\frac{f(x)\,\varphi(x)}{g(x)\,\psi(x)} = \frac{f_0(x)\,\varphi_0(x)}{g_0(x)\,\psi_0(x)}.$$

Ainsi, par analogie avec la définition de la somme de classes donnée ci-dessus, on peut parler du *produit* de classes de fractions égales.

La *commutativité* et l'*associativité* de cette multiplication résultent immédiatement de (3), tandis que la *loi de distributivité* se démontre de la manière suivante:

$$\left[\frac{f(x)}{g(x)} + \frac{\varphi(x)}{\psi(x)}\right]\frac{u(x)}{v(x)} = \frac{f(x)\,\psi(x) + g(x)\,\varphi(x)}{g(x)\,\psi(x)} \cdot \frac{u(x)}{v(x)} =$$
$$= \frac{[f(x)\,\psi(x) + g(x)\,\varphi(x)]\,u(x)}{g(x)\,\psi(x)\,v(x)} = \frac{f(x)\,\psi(x)\,u(x) + g(x)\,\varphi(x)\,u(x)}{g(x)\,\psi(x)\,v(x)} =$$
$$= \frac{f(x)\,\psi(x)\,u(x)\,v(x) + g(x)\,\varphi(x)\,u(x)\,v(x)}{g(x)\,\psi(x)\,v^2(x)} =$$
$$= \frac{f(x)\,u(x)}{g(x)\,v(x)} + \frac{\varphi(x)\,u(x)}{\psi(x)\,v(x)} = \frac{f(x)}{g(x)} \cdot \frac{u(x)}{v(x)} + \frac{\varphi(x)}{\psi(x)} \cdot \frac{u(x)}{v(x)}.$$

Il est facile de voir que les fractions de la forme $\frac{f(x)}{f(x)}$, c'est-à-dire les fractions de numérateur égal au dénominateur, sont toutes égales et forment une classe. Cette classe est appelée *classe unité* et tient

le rôle de l'élément unité pour la multiplication définie ci-dessus:

$$\frac{f(x)}{f(x)}\cdot\frac{\varphi(x)}{\psi(x)}=\frac{f(x)\,\varphi(x)}{f(x)\,\psi(x)}=\frac{\varphi(x)}{\psi(x)}.$$

Enfin, si une fraction $\frac{f(x)}{g(x)}$ n'appartient pas à la classe nulle, c'est-à-dire $f(x)\neq 0$, alors la fraction $\frac{g(x)}{f(x)}$ existe. Etant donné l'égalité

$$\frac{f(x)}{g(x)}\cdot\frac{g(x)}{f(x)}=\frac{f(x)\,g(x)}{g(x)\,f(x)},$$

et vu que le second membre de cette égalité appartient à la classe unité, la classe des fractions égales à $\frac{g(x)}{f(x)}$ est une classe *inverse* de celle contenant les fractions égales à $\frac{f(x)}{g(x)}$. Il en résulte l'existence de la division bien définie.

Ainsi, *l'ensemble des classes de fractions rationnelles égales, à coefficients dans un champ P, muni des opérations algébriques définies ci-dessus, forme un champ commutatif.* Il coïncide avec le champ cherché $P(x)$. D'ailleurs, il nous reste encore à démontrer que le champ trouvé contient un sous-anneau isomorphe à l'anneau $P[x]$ et que tout élément du champ est un quotient de deux éléments de ce sous-anneau.

Faisant correspondre à tout polynôme $f(x)$ de l'anneau $P[x]$ la classe des fractions rationnelles égales à $\frac{f(x)}{1}$ (bien entendu, l'ensemble des fractions contient, en particulier, les fractions ayant l'unité pour dénominateur), nous obtenons une application bijective de l'anneau $P[x]$ sur une partie du champ construit. En effet, l'égalité

$$\frac{f(x)}{1}=\frac{\varphi(x)}{1}$$

aurait pour conséquence $f(x)\cdot 1=1\cdot\varphi(x)$ ou, encore, $f(x)=\varphi(x)$. De plus, cette application est un isomorphisme, comme le montrent les égalités:

$$\frac{f(x)}{1}+\frac{g(x)}{1}=\frac{f(x)\cdot 1+g(x)\cdot 1}{1^2}=\frac{f(x)+g(x)}{1},$$

$$\frac{f(x)}{1}\cdot\frac{g(x)}{1}=\frac{f(x)\cdot g(x)}{1}.$$

Ainsi, *les classes des fractions de la forme* $\frac{f(x)}{1}$ *forment un sous-anneau du champ construit, qui est isomorphe à l'anneau* $P[x]$. On peut, donc, noter une fraction $\frac{f(x)}{1}$ par $f(x)$ tout court. Enfin, une

classe des fractions égales à $\frac{1}{g(x)}$ avec $g(x) \neq 0$ étant l'inverse de la classe des fractions égales à $\frac{g(x)}{1}$, il résulte de l'égalité

$$\frac{f(x)}{1} \cdot \frac{1}{g(x)} = \frac{f(x)}{g(x)}$$

que les *éléments du champ construit peuvent être considérés comme quotients* (dans le sens de la division définie sur ce champ) *de deux polynômes de l'anneau* $P[x]$.

Nous avons construit le champ des fractions rationnelles $P(x)$ sur un champ P quelconque. Utilisant la même méthode et remplaçant l'anneau des polynômes par l'anneau des nombres entiers, on peut construire le champ des nombres rationnels. Partant de ces deux exemples et utilisant la même méthode, on pourrait démontrer le théorème suivant: tout anneau commutatif sans diviseurs de zéro est un sous-anneau d'un champ.

Chapitre XI

POLYNÔMES DE PLUSIEURS INDÉTERMINÉES

§ 51. Anneau des polynômes de plusieurs indéterminées

Il arrive souvent qu'on doive considérer des polynômes dépendant non pas d'une indéterminée, mais de deux, trois et, plus généralement, de plusieurs indéterminées. Ainsi, nous avons déjà étudié dans les premiers chapitres du livre les formes linéaires et quadratiques qui sont des exemples de tels polynômes. De façon générale, on appelle *polynôme de n indéterminées* $x_1, x_2, \ldots, x_n$ *sur un champ P et on le note* $f(x_1, x_2, \ldots, x_n)$ une somme finie de termes de la forme $x_1^{k_1}, x_2^{k_2}, \ldots, x_n^{k_n}$, avec $k_i \geqslant 0$, à coefficients dans le champ P; bien entendu, on suppose que la somme exprimant le polynôme $f(x_1, x_2, \ldots, x_n)$ ne contienne pas de termes semblables et que les termes précédés de coefficients nuls ne soient pas pris en considération. Deux polynômes de n indéterminées, $f(x_1, x_2, \ldots, x_n)$ et $g(x_1, x_2, \ldots, x_n)$, *coïncident* (ou sont identiques) si les termes semblables dans leurs expressions ont les mêmes coefficients.

Soit un polynôme $f(x_1, x_2, \ldots, x_n)$ sur un champ P; le *degré de f en l'indéterminée* x_i, $i = 1, 2, \ldots, n$, est l'exposant le plus élevé de x_i intervenant dans l'expression de f. Il peut arriver éventuellement que ce degré soit 0; cela signifie que l'indéterminée x_i n'intervient pas dans l'expression de f, quoiqu'on considère f comme un polynôme de n indéterminées $x_1, x_2, \ldots, x_n$.

D'autre part, appelant *degré du terme*

$$x_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}$$

le nombre $k_1 + k_2 + \ldots + k_n$, c'est-à-dire la somme des exposants des indéterminées, le *degré d'un polynôme* $f(x_1, x_2, \ldots, x_n)$ (c'est-à-dire le degré de f par rapport à l'ensemble des indéterminées) est le degré le plus élevé de ses termes.

En particulier, tout comme dans le cas d'une indéterminée, les polynômes de degré nul coïncident avec les éléments non nuls du champ P et le polynôme nul est le seul polynôme de n indéterminées dont le degré ne soit pas défini. Il est clair que généralement un polynôme peut avoir plusieurs termes de degré le plus élevé et l'on ne peut plus parler d'un terme principal d'un polynôme (du point de vue du degré de ce polynôme).

On définit de la manière suivante les opérations d'addition et de multiplication pour les polynômes de n indéterminées sur un champ P. On appelle *somme* de deux polynômes $f(x_1, x_2, \ldots, x_n)$ et $g(x_1, x_2, \ldots, x_n)$ le polynôme à coefficients sommes des coefficients des termes semblables des polynômes f et g; évidemment, si un terme du polynôme f n'a pas de terme semblable dans l'expression de g, alors on considère que ce terme est précédé du coefficient nul dans l'expression de g; on admet la même convention pour tout terme de g n'ayant pas de termes semblables dans l'expression de f. Le produit de deux « monômes » est défini par la formule

$$ax_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}\cdot bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n}=(ab)\,x_1^{k_1+l_1}x_2^{k_2+l_2}\ldots x_n^{k_n+l_n};$$

ceci étant, on définit le *produit* de deux polynômes $f(x_1, x_2, \ldots, x_n)$ et $g(x_1, x_2, \ldots, x_n)$ en multipliant terme à terme et en groupant ensuite les termes semblables.

L'ensemble des polynômes de n indéterminées sur un champ P, muni des opérations définies ci-dessus, devient un anneau commutatif; en outre, cet anneau ne possède pas de diviseurs de zéro. En effet, pour $n = 1$ nos définitions coïncident avec celles données au § 20 dans le cas des polynômes d'une indéterminée. Supposons que les polynômes de $n - 1$ indéterminées à coefficients dans un champ P forment un anneau sans diviseurs de zéro. Tout polynôme de n indéterminées $x_1, x_2, \ldots, x_n$ peut être représenté d'une façon unique sous forme de polynôme de l'indéterminée x_n dont les coefficients sont des polynômes de $x_1, x_2, \ldots, x_{n-1}$; réciproquement, tout polynôme de x_n dont les coefficients sont des éléments de l'anneau des polynômes de $x_1, x_2, \ldots, x_{n-1}$ sur un champ P peut être considéré comme un polynôme sur le champ P dépendant de l'ensemble des indéterminées $x_1, x_2, \ldots, x_{n-1}, x_n$. On vérifie aisément que l'application bijective établie entre les polynômes de n indéterminées et les polynômes d'une indéterminée sur l'anneau des polynômes de $n - 1$ indéterminées est un isomorphisme par rapport aux opérations d'addition et de multiplication. A présent, notre proposition résulte du fait que les polynômes d'une indéterminée sur l'anneau des polynômes de $n - 1$ indéterminées forment un anneau; en outre, cet anneau, en tant qu'anneau des polynômes d'une indéterminée sur un anneau sans diviseurs de zéro, ne contient pas non plus de diviseurs de zéro (cf. § 47).

Nous avons donc démontré l'existence d'un *anneau des polynômes de n indéterminées sur un champ P*; cet anneau est noté par le symbole $P[x_1, x_2, \ldots, x_n]$.

Les considérations qui suivent permettent de considérer un anneau des polynômes de n indéterminées sous un autre angle. Supposons que le champ P soit un sous-anneau d'un anneau commutatif L. Choisissons dans L n éléments, soit $\alpha_1, \alpha_2, \ldots, \alpha_n$, et trouvons

un sous-anneau minimal L' de l'anneau L, contenant les éléments choisis et le champ P, c'est-à-dire formons un sous-anneau qui s'obtient par *adjonction* au champ P des éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$. Le sous-anneau L' se compose des éléments de l'anneau L qui s'expriment par les éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$ et ceux du champ P au moyen de l'addition, de la soustraction et de la multiplication. Il est facile de voir que ce sont exactement ceux des éléments de l'anneau L qui peuvent être représentés (au moyen des opérations dans L) sous forme de polynômes de $\alpha_1, \alpha_2, \ldots, \alpha_n$ à coefficients dans P; en outre, l'addition et la multiplication de ces éléments, en tant qu'éléments de L, se font d'après les règles d'addition et de multiplication des polynômes de n indéterminées indiquées ci-dessus.

Evidemment, un élément donné β du sous-anneau L' peut avoir, dans le cas général, plusieurs écritures sous forme d'un polynôme de $\alpha_1, \alpha_2, \ldots, \alpha_n$ à coefficients dans P. Si pour tout β de L' une telle écriture est *unique*, c'est-à-dire si des polynômes de $\alpha_1, \alpha_2, \ldots, \alpha_n$ distincts sont des éléments distincts de l'anneau L' (et, par conséquent, de l'anneau L), alors la famille des éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$ est dite *algébriquement indépendante* sur le champ P; dans le cas contraire, cette famille est dite *algébriquement dépendante* [1]. On peut en déduire la conclusion suivante:

Soient un champ P, sous-anneau d'un anneau commutatif L, et une famille des éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$ de L algébriquement indépendante sur P; alors le sous-anneau L' (de l'anneau L), engendré par adjonction au champ P des éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$, est isomorphe à l'anneau des polynômes $P[x_1, x_2, \ldots, x_n]$.

Parmi les autres propriétés de l'anneau des polynômes de n indéterminées $P[x_1, x_2, \ldots, x_n]$ indiquons encore la propriété suivante: on peut inclure l'anneau $P[x_1, x_2, \ldots, x_n]$ dans le *champ des fractions rationnelles $P(x_1, x_2, \ldots, x_n)$ de n indéterminées sur le champ P*. Tout élément de ce champ peut être écrit sous la forme $\frac{f}{g}$ avec f et g éléments de l'anneau $P[x_1, x_2, \ldots, x_n]$; en outre, $\frac{f}{g} = \frac{\varphi}{\psi}$ si et seulement si $f\psi = g\varphi$. L'addition et la multiplication de ces fractions s'effectuent d'après les règles qui sont valables pour les quotients dans tout champ, comme il l'a été indiqué au § 45. La démonstration de l'existence du champ $P(x_1, x_2, \ldots, x_n)$ peut être faite de la même manière qu'au § 50 pour $n = 1$.

---

[1] Les notions correspondantes pour $n = 1$ ont été déjà introduites au § 47: un élément α, algébriquement indépendant sur un champ P au sens de la définition donnée ici, a été appelé au § 47 *transcendant* sur P (dans le cas de dépendance algébrique, α a été appelé *algébrique* sur P).

La théorie de divisibilité des polynômes d'une indéterminée étudiée dans les chapitres V et X peut être développée et généralisée pour les polynômes de n indéterminées. Cependant, n'ayant pas pour but une étude détaillée de l'anneau des polynômes de plusieurs indéterminées, nous nous bornerons ici à la considération des problèmes concernant la décomposition d'un polynôme en facteurs irréductibles.

Introduisons d'abord la notion suivante: un polynôme $f(x_1, x_2, \ldots, x_n)$ dont tous les termes sont de même degré s est appelé *polynôme homogène* ou, encore, *forme* de degré s. On a déjà étudié les formes *linéaires* et *quadratiques*; on peut aussi considérer les *formes cubiques* dont tous les termes sont de degré 3 par rapport à l'ensemble des indéterminées, etc. *Tout polynôme de n indéterminées peut être représenté de façon unique sous forme de somme d'un certain nombre de polynômes homogènes de degrés différents*: pour obtenir une telle représentation il suffit de grouper les termes de même degré. Ainsi, le polynôme du quatrième degré $f(x_1, x_2, x_3) = 3x_1x_2^2 - 7x_1^2x_2^2 + x_2 - 5x_1x_2x_3 + x_1^4 - 2x_3 - 6 + x_3^3$ est la somme de la forme du quatrième degré $x_1^4 - 7x_1^2x_2^2$, de la forme cubique $3x_1x_2^2 - 5x_1x_2x_3 + x_3^3$, de la forme linéaire $x_2 - 2x_3$ et de la forme -6 (forme de degré nul).

Démontrons maintenant le *théorème*:

Le degré du produit de deux polynômes non nuls de n indéterminées est égal à la somme des degrés des polynômes.

Supposons d'abord que nous ayons deux *formes*, soit $\varphi(x_1, x_2, \ldots, x_n)$ de degré s et $\psi(x_1, x_2, \ldots, x_n)$ de degré t. Le produit d'un terme de la forme φ et d'un terme de la forme ψ est, manifestement, de degré $s + t$, de sorte que le produit $\varphi\psi$ est une somme de termes de degré $s + t$, car, groupant les termes semblables, on ne peut pas annuler tous les coefficients du produit, vu l'absence de diviseurs de zéro dans l'anneau $P[x_1, x_2, \ldots, x_n]$.

Soient maintenant deux polynômes $f(x_1, x_2, \ldots, x_n)$ de degré s et $g(x_1, x_2, \ldots, x_n)$ de degré t. Représentant f et g comme sommes de formes de degrés différents, on obtient:

$$f(x_1, x_2, \ldots, x_n) = \varphi(x_1, x_2, \ldots, x_n) + \ldots,$$
$$g(x_1, x_2, \ldots, x_n) = \psi(x_1, x_2, \ldots, x_n) + \ldots,$$

où φ et ψ sont des formes de degrés respectivement s et t et les points de suspension désignent des formes de degrés inférieurs respectivement à s et à t. Alors

$$fg = \varphi\psi + \ldots;$$

d'après ce qui vient d'être démontré, la forme $\varphi\psi$ est de degré $s + t$; les degrés des termes désignés par les points de suspension étant inférieurs à $s + t$, le degré du produit fg est $s + t$. Le théorème est démontré.

Un polynôme φ est un *diviseur* d'un polynôme f (ou f est *divisible par* φ) s'il existe dans l'anneau $P[x_1, x_2, \ldots, x_n]$ un polynôme ψ tel que $f = \varphi\psi$. Il est facile de voir que les propriétés de divisibilité I-IX du § 21 sont conservées dans le cas général considéré. Un polynôme f de degré k, $k \geqslant 1$, est dit *réductible* sur un champ P s'il se décompose en un produit de polynômes de l'anneau $P[x_1, x_2, \ldots, x_n]$ de degrés inférieurs à k; dans le cas contraire f est dit *irréductible*.

Tout polynôme de l'anneau $P[x_1, x_2, \ldots, x_n]$ de degré non nul se décompose en un produit de facteurs irréductibles. Cette décomposition est unique à des facteurs de degré nul près.

Ce théorème généralise les résultats correspondants du § 48 concernant les polynômes d'une indéterminée. Sa première partie se démontre en répétant littéralement les raisonnements du § 48. La démonstration de la seconde partie est plus difficile. Avant de passer à cette démonstration, notons que la seconde

partie du théorème a pour conséquence la proposition suivante: *si le produit de deux polynômes f et g de l'anneau $P[x_1, x_2, \ldots, x_n]$ est divisible par un polynôme irréductible p, alors, au moins un des facteurs f et g est divisible par p.* En effet, supposant le contraire, nous obtiendrions pour le produit fg deux décompositions différentes en facteurs irréductibles, l'une contenant p et l'autre ne le contenant pas.

Raisonnons par récurrence sur le nombre d'indéterminées. Le théorème étant vrai pour $n = 1$, supposons qu'il soit déjà démontré pour les polynômes de n indéterminées. Nous voulons le démontrer pour tout polynôme φ de $(n + 1)$ indéterminées $x, x_1, x_2, \ldots, x_n$. Ecrivons ce polynôme sous la forme $\varphi(x)$; les coefficients de $\varphi(x)$ sont, donc, des polynômes de $x_1, x_2, \ldots, x_n$. Pour ces polynômes, en vertu de l'hypothèse de récurrence, le théorème est vrai, c'est-à-dire chacun de ces polynômes se décompose de façon unique en un produit de facteurs irréductibles. Appelons un polynôme $\varphi(x)$ *primitif* (plus précisément, polynôme *primitif sur l'anneau $P[x_1, x_2, \ldots, x_n]$*) si ses coefficients n'ont pas de facteurs irréductibles communs, c'est-à-dire si les coefficients de $\varphi(x)$ forment une famille de polynômes réciproquement premiers; démontrons le lemme de Gauss:

Le produit de deux polynômes primitifs est un polynôme primitif.

En effet, soient deux polynômes primitifs à coefficients dans l'anneau $P[x_1, x_2, \ldots, x_n]$:

$$f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_ix^{k-i} + \ldots + a_k,$$
$$g(x) = b_0x^l + b_1x^{l-1} + \ldots + b_jx^{l-j} + \ldots + b_l$$

et soit

$$f(x)\,g(x) = c_0x^{k+l} + c_1x^{k+l-1} + \ldots + c_{i+j}x^{k+l-(i+j)} + \ldots + c_{k+l}.$$

Si ce produit n'est pas primitif, alors les coefficients $c_0, c_1, \ldots, c_{k+l}$ possèdent au moins un facteur irréductible commun, soit $p = p(x_1, x_2, \ldots, x_n)$. Les coefficients du polynôme primitif $f(x)$ n'étant pas tous divisibles par p, soit a_i le premier de ces coefficients qui n'ait pas p pour facteur; de même, désignons par b_j le premier des coefficients du polynôme $g(x)$ qui ne soit pas divisible par p. Multipliant terme à terme $f(x)$ et $g(x)$ et groupant les termes semblables contenant $x^{k+l-(i+j)}$, nous obtenons:

$$c_{i+j} = a_ib_j + a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \ldots + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \ldots$$

Le premier membre de cette égalité est divisible par le polynôme irréductible p. Il en est de même pour tous les termes du second membre, excepté le premier; en effet, vu les conditions imposées sur le choix des indices i et j, les coefficients $a_{i-1}, a_{i-2}, \ldots$ et $b_{j-1}, b_{j-2}, \ldots$ sont divisibles par p. Il en résulte que le produit a_ib_j l'est également, de sorte que, comme il l'a été montré ci-dessus, au moins un des facteurs a_i, b_j est divisible par p, ce qui n'est pas vrai. Ceci achève la démonstration du lemme de Gauss sous l'hypothèse de récurrence que notre théorème soit vrai pour les polynômes de n indéterminées.

On sait que l'anneau $P[x_1, x_2, \ldots, x_n]$ appartient au champ des fractions rationnelles $P(x_1, x_2, \ldots, x_n)$ que nous noterons par Q:

$$Q = P(x_1, x_2, \ldots, x_n).$$

Considérons l'anneau des polynômes $Q[x]$. Si un polynôme $\varphi(x)$ appartient à cet anneau, alors ses coefficients sont des quotients de polynômes de l'anneau $P[x_1, x_2, \ldots, x_n]$. Mettant en facteur le dénominateur commun de ces quotients, puis les facteurs communs des numérateurs, on peut représenter $\varphi(x)$ sous la forme

$$\varphi(x) = \frac{a}{b} f(x).$$

Ici a et b sont des polynômes de l'anneau $P[x_1, x_2, \ldots, x_n]$ et $f(x)$ est un polynôme de x à coefficients dans $P[x_1, x_2, \ldots, x_n]$; de plus, $f(x)$ est un polynôme primitif, car ses coefficients n'ont pas de facteurs communs.

De cette manière on fait correspondre à tout polynôme $\varphi(x)$ de l'anneau $Q[x]$ un polynôme primitif $f(x)$. *Pour tout $\varphi(x)$ le polynôme correspondant $f(x)$ est bien défini à un facteur non nul dans le champ P près.* En effet, soit

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x),$$

où $g(x)$ est encore un polynôme primitif. Alors

$$adf(x) = bcg(x).$$

Ainsi, ad et bc sont obtenus en mettant en facteur les diviseurs communs des coefficients d'un même polynôme sur l'anneau $P[x_1, x_2, \ldots, x_n]$. Le théorème d'unicité de la décomposition en facteurs irréductibles étant supposé vrai pour les polynômes de n indéterminées (hypothèse de récurrence), il en résulte que ad et bc doivent coïncider à un facteur de degré nul près. Par conséquent, les polynômes primitifs $f(x)$ et $g(x)$ coïncident au même facteur de degré nul près.

Au produit de deux polynômes de l'anneau $Q[x]$ on peut associer le produit de deux polynômes primitifs correspondants. En effet, soient

$$\varphi(x) = \frac{a}{b} f(x), \qquad \psi(x) = \frac{c}{d} g(x),$$

où $f(x)$ et $g(x)$ sont primitifs; alors

$$\varphi(x)\psi(x) = \frac{ac}{bd} f(x) g(x).$$

Or on a démontré ci-dessus que le produit $f(x) g(x)$ est un polynôme primitif.

Notons ensuite que *si un polynôme $\varphi(x)$ de l'anneau $Q[x]$ est irréductible sur le champ Q, alors le polynôme primitif correspondant $f(x)$, en tant que polynôme de $x, x_1, x_2, \ldots, x_n$, l'est aussi; la réciproque est aussi vraie.* En effet, supposons que le polynôme f soit réductible, $f = f_1 f_2$; alors les deux facteurs f_1 et f_2 doivent dépendre de x, car, dans le cas contraire, f ne serait pas primitif. Il en découle la décomposition du polynôme $\varphi(x)$ sur le champ Q:

$$\varphi(x) = \frac{a}{b} f(x) = \left(\frac{a}{b} f_1\right) f_2.$$

Inversement, si le polynôme $\varphi(x)$ est réductible sur Q, $\varphi(x) = \varphi_1(x)\varphi_2(x)$, alors les polynômes primitifs correspondants $f_1(x)$ et $f_2(x)$ dépendent tous les deux de x; or on a démontré ci-dessus que leur produit est égal à $f(x)$ (à un facteur du champ P près).

Soit maintenant un polynôme primitif f; décomposons f en facteurs irréductibles: $f = f_1 \cdot f_2 \ldots f_k$. Non seulement chacun de ces facteurs dépend de x, mais il est aussi un polynôme primitif, car, dans le cas contraire, f ne serait pas primitif. *Cette décomposition d'un polynôme primitif est bien définie à des facteurs, éléments non nuls de P, près.* En effet, vu le lemme précédent, on peut considérer cette décomposition comme la décomposition de $f(x)$ en facteurs irréductibles sur le champ Q; or, pour les polynômes d'une indéterminée sur un champ quelconque l'unicité de la décomposition en facteurs irréductibles a été déjà démontrée; cette unicité a lieu à un facteur de Q près; cependant, dans notre cas, vu que les facteurs f_i sont primitifs, l'unicité de la décomposition en facteurs irréductibles a lieu à des facteurs, éléments non nuls de P, près.

Ces lemmes étant établis en partant de l'hypothèse de récurrence sur le nombre d'indéterminées, la démonstration du théorème énoncé ci-dessus se fait

sans aucune difficulté. En effet, tout polynôme irréductible de l'anneau $P[x, x_1, x_2, \ldots, x_n]$ est soit un polynôme irréductible de l'anneau $P[x_1, x_2, \ldots, x_n]$, soit un polynôme primitif irréductible. Il en résulte que quelle que soit la décomposition d'un polynôme $\varphi(x, x_1, x_2, \ldots, x_n)$ en facteurs irréductibles, on peut, en groupant convenablement les facteurs, mettre φ sous la forme

$$\varphi(x, x_1, x_2, \ldots, x_n) = a(x_1, x_2, \ldots, x_n) f(x, x_1, x_2, \ldots, x_n),$$

où a ne dépend pas de x et f est un polynôme primitif. Or, on sait que cette représentation de φ est unique à des facteurs, éléments de P, près. D'autre part, l'unicité de la décomposition en facteurs irréductibles étant vraie pour le polynôme a de n indéterminées en vertu de l'hypothèse de récurrence et pour le polynôme primitif f d'après le lemme précédent, le théorème énoncé est également démontré dans le cas des polynômes de $n + 1$ indéterminées.

Des lemmes démontrés ci-dessus il découle un autre corollaire intéressant: *si un polynôme $\varphi(x)$ à coefficients dans $P[x_1, x_2, \ldots, x_n]$ est réductible sur le champ $Q = P(x_1, x_2, \ldots, x_n)$, alors $\varphi(x)$ peut être décomposé en facteurs dépendant de x et ayant pour coefficients des polynômes de l'anneau $P[x_1, x_2, \ldots, x_n]$.* En effet, soit $f(x)$ le polynôme primitif correspondant à un polynôme $\varphi(x)$, c'est-à-dire $\varphi(x) = af(x)$; alors, on sait qu'une décomposition de $\varphi(x)$ entraîne celle de $f(x)$; mais cette dernière conduit à la décomposition de $\varphi(x)$ sur l'anneau $P[x_1, x_2, \ldots, x_n]$.

Différemment du cas des polynômes d'une indéterminée qui peuvent être décomposés en facteurs linéaires sur une extension convenablement choisie d'un champ de base donné (cf. § 49), *il existe pour tout champ P des polynômes de degré quelconque de plusieurs indéterminées* (égales ou supérieures à deux) *tels qu'ils soient a b s o l u m e n t i r r é d u c t i b l e s*, c'est-à-dire des polynômes tels qu'ils restent irréductibles quelle que soit l'extension du champ de base P.

Tel est, par exemple, le polynôme

$$f(x, y) = \varphi(x) + y,$$

où $\varphi(x)$ est un polynôme quelconque d'une indéterminée sur un champ P. En effet, s'il existait une extension de P, soit $\overline{P}$, telle que la décomposition

$$f(x, y) = g(x, y)\, h(x, y)$$

ait lieu, alors, écrivant g et h suivant les puissances de y, nous aurions, par exemple, que

$$g(x, y) = a_0(x)\, y + a_1(x), \quad h(x, y) = b_0(x),$$

c'est-à-dire que h ne dépend pas de y, puis, vu l'égalité $a_0(x)\, b_0(x) = 1$, que $b_0(x)$ est de degré nul, c'est-à-dire que h ne dépend pas de x non plus.

Ordre lexicographique des termes d'un polynôme. Il y a deux façons naturelles d'ordonner les termes des polynômes d'une indéterminée, à savoir suivant les puissances décroissantes et suivant les puissances croissantes de l'indéterminée. Il n'en est pas ainsi pour les polynômes de plusieurs indéterminées; par exemple, soit un polynôme du cinquième degré de trois indéterminées:

$$f(x_1, x_2, x_3) = x_1x_2^2x_3^2 + x_1^4x_3 + x_2^3x_3^2 + x_1^2x_2x_3^2,$$

on peut aussi l'écrire sous la forme

$$f(x_1, x_2, x_3) = x_1^4x_3 + x_1^2x_2x_3^2 + x_1x_2^2x_3^2 + x_2^3x_3^2,$$

et il n'y a pas de raisons de préférer l'une de ces écritures à l'autre. Néanmoins, il existe une façon bien définie d'ordonner les termes d'un polynôme de plusieurs indéterminées, quoiqu'elle dépende du choix de l'énumération des indéterminées ; pour les polynômes d'une indéterminée elle donne l'écriture suivant les puissances décroissantes de l'indéterminée. Cette façon d'ordonner les termes, dite *lexicographique*, est suggérée par la méthode usuelle d'ordonner les mots dans un dictionnaire (dans un « lexique ») : les lettres étant ordonnées suivant l'ordre alphabétique, on définit la place des mots dans un dictionnaire par leur première lettre ; deux mots ayant les mêmes premières lettres, on définit leurs places respectives par les lettres qui suivent immédiatement les premières lettres, etc.

Soient un polynôme $f(x_1, x_2, \ldots, x_n)$ de l'anneau $P[x_1, x_2, \ldots, x_n]$ et deux termes différents de f:

$$x_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}, \tag{1}$$

$$x_1^{l_1}x_2^{l_2} \ldots x_n^{l_n}, \tag{2}$$

précédés de coefficients, éléments non nuls du champ P. Les termes (1) et (2) étant distincts, au moins l'une des différences des exposants des indéterminées

$$k_i - l_i, \qquad i = 1, 2, \ldots, n,$$

est non nulle. Le terme (1) est dit *supérieur* au terme (2) (et le terme (2) est dit *inférieur* à (1)) si la première des différences non nulles est positive, c'est-à-dire s'il existe un indice i, $1 \leqslant i \leqslant n$, tel que

$$k_1 = l_1, \; k_2 = l_2, \; \ldots, \; k_{i-1} = l_{i-1}, \quad \text{mais} \quad k_i > l_i.$$

Autrement dit, le terme (1) est supérieur au terme (2) si l'exposant de x_1 dans (1) est supérieur à l'exposant de x_1 dans (2) ou si, les exposants de x_1 étant les mêmes, l'exposant de x_2 dans (1) est plus grand que l'exposant de x_2 dans (2), etc. Il est facile de voir que, le terme (1) étant supérieur au terme (2), cela ne signifie nullement que le degré du terme (1) par rapport à l'ensemble des indéterminées soit supérieur à celui du terme (2) ; en effet, des deux termes

$$x_1^3x_2x_3, \qquad x_1x_2^5x_3^2$$

le premier est supérieur bien qu'il soit de degré inférieur.

Il est clair que pour tout couple de termes distincts d'un polynôme $f(x)$ l'un est supérieur à l'autre. Il est également facile de vérifier que si le terme (1) est supérieur au terme (2) et le terme (2) au terme

$$x_1^{m_1}x_2^{m_2} \ldots x_n^{m_n}, \tag{3}$$

c'est-à-dire s'il existe un indice j, $1 \leqslant j \leqslant n$, tel que

$$l_1 = m_1, \; l_2 = m_2, \; \ldots, \; l_{j-1} = m_{j-1}, \quad \text{mais} \quad l_j > m_j,$$

alors le terme (1) est supérieur au terme (3), et cela indépendamment du fait que i soit plus grand, égal ou plus petit que j. Ainsi, ordonnant les termes d'un polynôme suivant l'ordre de décroissance défini ci-dessus, nous obtenons un ordre bien défini des termes du polynôme $f(x_1, x_2, \ldots, x_n)$ dit ordre lexicographique.

Ainsi, le polynôme

$$f(x_1, x_2, x_3, x_4) = x_1^4 + 3x_1^2x_2^3x_3 - x_1^2x_2^3x_4^2 + 5x_1x_3x_4^2 + 2x_2 + x_3^3x_4 - 4$$

est écrit suivant l'ordre lexicographique.

Un polynôme $f(x_1, x_2, \ldots, x_n)$ étant écrit suivant l'ordre lexicographique, un de ses termes occupe la première place, c'est-à-dire il est supérieur à tous les autres termes. Nous l'appelons le *plus haut terme du polynôme*; dans l'exemple précédent le terme x_1^4 était le plus haut. Nous allons démontrer un *lemme* sur les plus hauts termes; ce lemme sera utilisé dans le paragraphe suivant.

Le plus haut terme du produit de deux polynômes de n indéterminées est égal au produit des plus hauts termes des facteurs.

En effet, soient deux facteurs $f(x_1, x_2, \ldots, x_n)$ et $g(x_1, x_2, \ldots, x_n)$. Soient

$$ax_1^{k_1}x_2^{k_2} \ldots x_n^{k_n}, \tag{4}$$

$$a'x_1^{s_1}x_2^{s_2} \ldots x_n^{s_n}, \tag{5}$$

respectivement le plus haut terme et un autre terme quelconque du polynôme $f(x_1, x_2, \ldots, x_n)$; alors il existe un indice i, $1 \leqslant i \leqslant n$, tel que

$$k_1 = s_1, \ldots, k_{i-1} = s_{i-1}, \qquad k_i > s_i.$$

D'autre part, soient

$$bx_1^{l_1}x_2^{l_2} \ldots x_n^{l_n}, \tag{6}$$

$$b'x_1^{t_1}x_2^{t_2} \ldots x_n^{t_n} \tag{7}$$

respectivement le plus haut terme et un autre terme quelconque du polynôme $g(x_1, x_2, \ldots, x_n)$; alors il existe un indice j, $1 \leqslant j \leqslant n$, tel que

$$l_1 = t_1, \ldots, l_{j-1} = t_{j-1}, \; l_j > t_j.$$

Multipliant les termes (4) et (6), ainsi que les termes (5) et (7), on obtient :

$$abx_1^{k_1+l_1}x_2^{k_2+l_2} \ldots x_n^{k_n+l_n}, \tag{8}$$

$$a'b'x_1^{s_1+t_1}x_2^{s_2+t_2} \ldots x_n^{s_n+t_n}. \tag{9}$$

Or, il est facile de voir que le terme (8) est supérieur au terme (9); si, par exemple, $i \leqslant j$, alors

$$k_1 + l_1 = s_1 + t_1, \ldots, k_{i-1} + l_{i-1} = s_{i-1} + t_{i-1}, \quad \text{mais} \quad k_i + l_i > s_i + t_i,$$

car $k_i > s_i$, $l_i \geqslant t_i$. On vérifie de la même manière que le terme (8) est supérieur au produit des termes (4) et (7) et à celui des termes (5)

et (6). Ainsi, le terme (8), produit des plus hauts termes des polynômes f et g, est supérieur à tout autre qui s'obtienne par la multiplication terme à terme des polynômes f et g; par conséquent, le terme (8) ne peut pas disparaître lorsque nous groupons les termes semblables, autrement dit, il est le plus haut terme du produit fg.

§ 52. Polynômes symétriques

Parmi les polynômes de plusieurs indéterminées se font distinguer ceux qui sont invariants par rapport aux permutations des indéterminées. Les indéterminées interviennent, donc, de façon symétrique dans l'expression de ces polynômes, c'est pourquoi ils sont dits *polynômes symétriques* (ou encore *fonctions symétriques*). Voici les plus simples exemples de tels polynômes: somme des indéterminées $x_1 + x_2 + \ldots + x_n$, somme des carrés des indéterminées $x_1^2 + x_2^2 + \ldots + x_n^2$, produit des indéterminées $x_1x_2 \ldots x_n$, etc. Vu que toute permutation de n éléments est un produit d'un nombre fini de transpositions (cf. § 3), il suffit, pour démontrer la symétrie d'un polynôme, de vérifier qu'il est invariant par rapport à toute transposition des indéterminées.

Par la suite nous considérerons les polynômes symétriques de n indéterminées à coefficients dans un champ P. Il est facile de voir que *la somme, la différence et le produit de deux polynômes symétriques sont des polynômes symétriques*, c'est-à-dire les polynômes symétriques forment un sous-anneau de l'anneau $P[x_1, x_2, \ldots, x_n]$ des polynômes de n indéterminées sur un champ P, dit *anneau des polynômes symétriques de n indéterminées sur un champ P*. Les éléments de P (c'est-à-dire les polynômes de degré nul et le polynôme nul) appartiennent manifestement à cet anneau, car ils sont invariants par rapport à toute permutation des indéterminées. Tout autre polynôme symétrique contient obligatoirement les n indéterminées et son degré en chaque indéterminée est le même; en effet, si un terme du polynôme symétrique $f(x_1, x_2, \ldots, x_n)$ contient l'indéterminée x_i à la puissance k, alors la transposition des indéterminées x_i et x_j dans ce terme donne encore un terme de f, qui contient x_j à la même puissance k.

Les polynômes symétriques de n indéterminées

$$\left.\begin{array}{l}
\sigma_1 = x_1 + x_2 + \ldots + x_n, \\
\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \\
\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\sigma_{n-1} = x_1x_2 \ldots x_{n-1} + x_1x_2 \ldots x_{n-2}x_n + \ldots + x_2x_3 \ldots x_n, \\
\sigma_n = x_1x_2 \ldots x_n
\end{array}\right\} \quad (1)$$

sont dits *polynômes symétriques élémentaires*. Ces polynômes (leur symétrie est évidente) jouent un grand rôle dans la théorie des polynômes symétriques. Ils sont suggérés par les formules de Viète (cf. § 24), de sorte que *les coefficients de tout polynôme d'une indéterminée, dont le coefficient du terme principal est l'unité, sont les fonctions symétriques élémentaires (au signe près) de ses zéros.* La relation entre les polynômes symétriques élémentaires et les formules de Viète est très importante pour les applications des polynômes symétriques à la théorie des polynômes d'une indéterminée; d'ailleurs, ce sont justement ces applications qui nous incitent à l'étude des polynômes symétriques.

Les polynômes symétriques de n indéterminées $x_1, x_2, \ldots, x_n$ sur un champ P formant un anneau, les propositions suivantes sont évidentes: un polynôme symétrique élémentaire élevé à une puissance entière positive ainsi que le produit de telles puissances, précédé d'un coefficient de P, sont les polynômes symétriques; il en est de même pour la somme finie de tels produits. Autrement dit, *tout polynôme des polynômes symétriques élémentaires* $\sigma_1, \sigma_2, \ldots$ $\ldots, \sigma_n$ *à coefficients dans P est symétrique, en tant que polynôme des indéterminées* $x_1, x_2, \ldots, x_n$. Ainsi, pour $n = 3$, soit le polynôme $\sigma_1\sigma_2 + 2\sigma_3$. Remplaçant σ_1, σ_2 et σ_3 par leurs expressions, il vient:

$$\sigma_1\sigma_2 + 2\sigma_3 = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 + 5x_1x_2x_3;$$

le second membre est manifestement un polynôme symétrique de x_1, x_2, x_3.

La réciproque de ce résultat est le *théorème fondamental de la théorie des polynômes symétriques*:

Tout polynôme symétrique de n indéterminées $x_1, x_2, \ldots, x_n$ sur un champ P est un polynôme des polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_n$ à coefficients dans P.

En effet, soit un polynôme symétrique

$$f(x_1, x_2, \ldots, x_n)$$

et supposons que son plus haut terme, suivant l'ordre lexicographique, soit

$$a_0x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n}. \qquad (2)$$

Les exposants des indéterminées dans le terme (2) doivent satisfaire aux inégalités

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_n. \qquad (3)$$

En effet, soit $k_i < k_{i+1}$ pour un certain indice i. Le polynôme $f(x_1, x_2, \ldots, x_n)$ étant symétrique, le terme qui s'obtient de (2)

par la transposition des indéterminées x_i et x_{i+1}, soit

$$a_0 x_1^{k_1} x_2^{k_2} \ldots x_i^{k_{i+1}} x_{i+1}^{k_i} \ldots x_n^{k_n}, \tag{4}$$

doit également intervenir dans l'expression de f. Cela nous conduit à une contradiction, car le terme (4) est, du point de vue de l'ordre lexicographique, supérieur au terme (2), les exposants des $x_1, x_2, \ldots, x_{i-1}$ étant les mêmes dans les deux termes et l'exposant de x_i dans (4) étant plus grand que celui dans (2).

Formons maintenant le produit des polynômes symétriques élémentaires:

$$\varphi_1 = a_0 \sigma_1^{k_1-k_2} \sigma_2^{k_2-k_3} \ldots \sigma_{n-1}^{k_{n-1}-k_n} \sigma_n^{k_n} \tag{5}$$

(vu les inégalités (3), les exposants dans (5) sont non négatifs). C'est un polynôme symétrique des indéterminées $x_1, x_2, \ldots, x_n$, dont le plus haut terme est (2). En effet, les plus hauts termes des polynômes $\sigma_1, \sigma_2, \ldots, \sigma_n$ sont respectivement $x_1, x_1x_2, x_1x_2x_3, \ldots, x_1x_2 \ldots x_n$; or, il a été montré dans le paragraphe précédent que le plus haut terme du produit est le produit des plus hauts termes des facteurs, de sorte que le plus haut terme de φ_1 est

$$a_0 x_1^{k_1-k_2} (x_1x_2)^{k_2-k_3} (x_1x_2x_3)^{k_3-k_4} \ldots (x_1x_2 \ldots x_{n-1})^{k_{n-1}-k_n} \times$$
$$\times (x_1x_2 \ldots x_n)^{k_n} = a_0 x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}.$$

Il en résulte que, retranchant φ_1 de f, le plus haut terme en disparaît, c'est-à-dire le plus haut terme du polynôme symétrique $f - \varphi_1 = f_1$ est inférieur au terme (2), qui est le plus haut terme de f. Appliquant ce même procédé au polynôme f_1, dont les coefficients sont encore des éléments du champ P, nous sommes conduits à l'égalité

$$f_1 = \varphi_2 + f_2,$$

où φ_2 est le produit de puissances de polynômes symétriques élémentaires muni d'un certain coefficient, élément de P, et f_2 est un polynôme symétrique dont le plus haut terme est inférieur à celui de f_1. Il en découle l'égalité

$$f = \varphi_1 + \varphi_2 + f_2.$$

Continuant ce processus, nous trouverons un entier positif s tel que $f_s = 0$, ce qui nous conduira à l'expression de f sous la forme d'un polynôme de $\sigma_1, \sigma_2, \ldots, \sigma_n$ à coefficients dans P:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{s} \varphi_i = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

En effet, supposant ce processus infini[1], nous obtiendrions une suite infinie de polynômes symétriques

$$f_1, f_2, \ldots, f_s, \ldots, \tag{6}$$

le plus haut terme du polynôme f_s étant inférieur à celui de f_{s-1}, $s = 2, 3, \ldots$, et, par conséquent, inférieur au terme (2). Or, le monôme

$$bx_1^{l_1}x_2^{l_2}\ldots x_n^{l_n} \tag{7}$$

étant le plus haut terme du polynôme f_s, la symétrie de f_s entraîne les inégalités analogues à (3) :

$$l_1 \geqslant l_2 \geqslant \ldots \geqslant l_n. \tag{8}$$

D'autre part, le terme (2) étant supérieur au terme (7), on a

$$k_1 \geqslant l_1. \tag{9}$$

Il est facile de voir qu'il n'existe qu'un nombre fini de façons dont on peut choisir les suites des entiers non négatifs $l_1, l_2, \ldots, l_n$ vérifiant les inégalités (8) et (9). En effet, renonçant même à l'inégalité (8) et supposant seulement des entiers non négatifs l_i, $i = 1, 2, \ldots, n$, bornés par l'entier k_1, le nombre de façons dont l_i peuvent être choisis est au plus $(k_1 + 1)^n$. Il en résulte que la suite des polynômes (6), dont les plus hauts termes forment une suite décroissante au sens lexicographique, ne peut pas être infinie.

La démonstration du théorème est terminée.

La relation entre les polynômes symétriques élémentaires et les formules de Viète signalée ci-dessus permet de déduire du théorème fondamental sur les polynômes symétriques une *conséquence* importante :

Soit un polynôme $f(x)$ d'une indéterminée sur un champ P ayant l'unité pour coefficients du terme principal. Alors tout polynôme symétrique (à coefficients dans P) des z é r o s *de $f(x)$, qui appartiennent à un champ de décomposition du polynôme $f(x)$ sur le champ P, est un polynôme (à coefficients dans P) des* c o e f f i c i e n t s *du polynôme $f(x)$ et, par conséquent, un élément du champ P.*

La démonstration du théorème fondamental donne aussi une méthode pratique de calcul de l'expression des polynômes symétriques par les polynômes symétriques élémentaires. Introduisons d'abord une notation: soit un produit de puissances des indéterminées $x_1, x_2, \ldots, x_n$ (dont quelques-unes peuvent

---

[1] Il faut prendre en considération que le polynôme φ_s contient, en général, des termes n'intervenant pas dans f_{s-1}, de sorte que le passage de f_{s-1} à $f_s = f_{s-1} - \varphi_s$ provoque non seulement la disparition de certains termes de f_{s-1}, mais aussi l'apparition de nouveaux termes, et cela pour tout s, $s = 1, 2, \ldots$

être d'exposant nul)

$$ax_1^{k_1}x_2^{k_2}\ \dots\ x_n^{k_n}; \qquad (10)$$

alors on note par

$$S\ (ax_1^{k_1}x_2^{k_2}\ \dots\ x_n^{k_n}) \qquad (11)$$

la somme des termes qui s'obtiennent de (10) par toutes les permutations des indéterminées. Il est clair que cette somme est un polynôme symétrique homogène et que tout polynôme symétrique de n indéterminées contenant le terme (10) contient, en même temps, tous les autres termes du polynôme (11). Par exemple, $S\ (x_1) = \sigma_1$, $S\ (x_1x_2) = \sigma_2$, $S\ (x_1^2)$ est la somme des carrés des indéterminées, etc.

Exemple. Exprimer le polynôme symétrique $f = S\ (x_1^2x_2)$ de n indéterminées en fonction des polynômes symétriques élémentaires.

Ici le plus haut terme est $x_1^2x_2$, de sorte que $\varphi_1 = \sigma_1^{2-1}\sigma_2 = \sigma_1\sigma_2$, c'est-à-dire

$$\varphi_1 = (x_1 + x_2 + \dots + x_n)(x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n) = \\ = S\ (x_1^2x_2) + 3S\ (x_1x_2x_3),$$

d'où on a

$$f_1 = f - \varphi_1 = -3S\ (x_1x_2x_3) = -3\sigma_3.$$

Ainsi, $f = \varphi_1 + f_1 = \sigma_1\sigma_2 - 3\sigma_3$.

Dans les cas plus compliqués il est logique de déterminer d'abord les termes qui peuvent intervenir dans l'expression du polynôme donné par les polynômes élémentaires et de trouver ensuite leurs coefficients par la méthode des coefficients indéterminés.

Exemples. 1. Trouver l'expression du polynôme symétrique $f = S\ (x_1^2x_2^2)$ en fonction des polynômes élémentaires.

On sait (cf. la démonstration du théorème fondamental) que les termes du polynôme cherché $\varphi\ (\sigma_1, \sigma_2, \dots, \sigma_n)$ sont déterminés par les plus hauts termes des polynômes symétriques $f_1, f_2, \dots$; en outre, ces plus hauts termes sont inférieurs au plus haut terme du polynôme f, soit le terme $x_1^2x_2^2$. Trouvons tous les produits de la forme $x_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ vérifiant les conditions : 1) ils sont inférieurs au terme $x_1^2x_2^2$, 2) ils peuvent être les plus hauts termes de certains polynômes symétriques, c'est-à-dire qu'ils satisfont aux inégalités $l_1 \geqslant l_2 \geqslant \dots \geqslant l_n$, 3) ils sont de degré 4 par rapport à l'ensemble des indéterminées (car on sait que tous les polynômes $f_1, f_2, \dots$ sont du même degré que le polynôme homogène f). N'écrivant que les combinaisons correspondantes des exposants et indiquant à côté les produits des puissances de σ_j définis par ces combinaisons, nous obtenons le tableau suivant :

$$22000 \dots \sigma_1^{2-2}\sigma_2^{2-0} = \sigma_2^2,$$
$$21100 \dots \sigma_1^{2-1}\sigma_2^{1-1}\sigma_3^{1-0} = \sigma_1\sigma_3,$$
$$11110 \dots \sigma_1^{1-1}\sigma_2^{1-1}\sigma_3^{1-1}\sigma_4^{1-0} = \sigma_4.$$

Ainsi, le polynôme f est de la forme

$$f = \sigma_2^2 + A\sigma_1\sigma_3 + B\sigma_4.$$

Le coefficient de σ_2 est l'unité, ce terme étant défini par le plus haut terme du polynôme f et, par conséquent, ayant le même coefficient (on le sait déjà de la démonstration du théorème fondamental). Trouvons les coefficients A et B.

Posons $x_1 = x_2 = x_3 = 1$, $x_4 = \ldots = x_n = 0$. Il est facile de voir que la valeur correspondante du polynôme f est 3, tandis que les valeurs des polynômes σ_1, σ_2, σ_3 et σ_4 sont respectivement 3, 3, 1 et 0. Par conséquent,

$$3 = 9 + A \cdot 3 \cdot 1 + B \cdot 0,$$

d'où $A = -2$. Faisant maintenant $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = \ldots = x_n = 0$, les valeurs correspondantes des polynômes f, σ_1, σ_2, σ_3 et σ_4 deviennent respectivement 6, 4, 6, 4, 1. Ainsi,

$$6 = 36 - 2 \cdot 4 \cdot 4 + B \cdot 1,$$

d'où $B = 2$. Par conséquent, l'expression cherchée de f est

$$f = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4.$$

2. Trouver la somme des cubes des zéros du polynôme

$$f(x) = x^4 + x^3 + 2x^2 + x + 1.$$

Afin de résoudre ce problème trouvons l'expression du polynôme symétrique $S(x_1^3)$ en fonction des polynômes symétriques élémentaires. Appliquant la même méthode que dans l'exemple précédent, nous obtenons le tableau:

$$3000 \ldots \sigma_1^3,$$
$$2100 \ldots \sigma_1\sigma_2,$$
$$1110 \ldots \sigma_3,$$

de sorte que

$$S(x_1^3) = \sigma_1^3 + A\sigma_1\sigma_2 + B\sigma_3.$$

Posant d'abord $x_1 = x_2 = 1$, $x_3 = \ldots = x_n = 0$, puis $x_1 = x_2 = x_3 = 1$, $x_4 = \ldots = x_n = 0$, nous obtenons $A = -3$, $B = 3$, c'est-à-dire

$$S(x_1^3) = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \tag{12}$$

Afin de calculer la somme des cubes des zéros du polynôme donné $f(x)$, il faut, vu les formules de Viète, remplacer dans l'expression trouvée ci-dessus σ_1 par le coefficient de x^3 avec le signe contraire, soit par -1, ensuite, remplacer σ_2 par le coefficient de x^2, c'est-à-dire par 2, et, enfin, remplacer σ_3 par le coefficient de x avec le signe contraire, soit par -1. Ainsi, la somme en question est

$$(-1)^3 - 3 \cdot (-1) \cdot 2 + 3 \cdot (-1) = 2.$$

Le polynôme $f(x)$ ayant pour zéros les nombres complexes $i, -i, -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ et $-\frac{1}{2} - i\frac{\sqrt{3}}{2}$, le lecteur peut vérifier ce résultat directement. De même, il est clair que la formule (12) ne dépend pas de $f(x)$ et permet de calculer la somme des cubes des zéros pour tout polynôme.

La méthode qui permet d'exprimer un polynôme symétrique f en fonction des polynômes symétriques élémentaires, donnée dans la démonstration du théorème fondamental, conduit à un polynôme de $\sigma_1, \sigma_2, \ldots, \sigma_n$ bien défini. Il se révèle que toute méthode conduit inévitablement à la même expression de f par $\sigma_1, \sigma_2, \ldots, \sigma_n$. On a le *théorème d'unicité* suivant:

Tout polynôme symétrique s'exprime de façon unique sous forme de polynôme des polynômes symétriques élémentaires.

Démontrons ce théorème. Soient deux expressions en fonction de $\sigma_1, \sigma_2, \ldots, \sigma_n$ d'un polynôme symétrique sur un champ P:

$$f(x_1, x_2, \ldots, x_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) = \psi(\sigma_1, \sigma_2, \ldots, \sigma_n);$$

alors la différence

$$\chi(\sigma_1, \sigma_2, \ldots, \sigma_n) = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n) - \psi(\sigma_1, \sigma_2, \ldots, \sigma_n)$$

est un polynôme non nul de $\sigma_1, \sigma_2, \ldots, \sigma_n$ (c'est-à-dire χ possède des coefficients non nuls); d'autre part, ce même polynôme avec $\sigma_1, \sigma_2, \ldots, \sigma_n$ remplacés par $x_1, x_2, \ldots, x_n$ (d'après les formules (1)) devient l'élément nul de l'anneau $P[x_1, x_2, \ldots, x_n]$. Ainsi, il reste à démontrer que pour tout polynôme non nul $\chi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ (c'est-à-dire χ possède au moins un coefficient non nul), le polynôme $g(x_1, x_2, \ldots, x_n)$, qui s'obtient de χ en substituant à $\sigma_1, \sigma_2, \ldots, \sigma_n$ leurs expressions (1) en fonction des $x_1, x_2, \ldots, x_n$:

$$\chi(\sigma_1, \sigma_2, \ldots, \sigma_n) = g(x_1, x_2, \ldots, x_n), \tag{13}$$

est également non nul.

Soit $a\sigma_1^{k_1}\sigma_2^{k_2} \ldots \sigma_n^{k_n}$ un des termes du polynôme χ, $a \neq 0$; alors, remplaçant $\sigma_1, \sigma_2, \ldots, \sigma_n$ par leurs expressions (1), nous obtenons un polynôme de $x_1, x_2, \ldots, x_n$ dont le plus haut terme (suivant l'ordre lexicographique) est, comme on sait déjà de la démonstration du théorème fondamental, le monôme:

$$ax_1^{k_1}(x_1x_2)^{k_2} \ldots (x_1x_2 \ldots x_n)^{k_n} = ax_1^{l_1}x_2^{l_2} \ldots x_n^{l_n},$$

avec

$$\begin{aligned} l_1 &= k_1 + k_2 + \ldots + k_n, \\ l_2 &= \phantom{k_1 + {}} k_2 + \ldots + k_n, \\ &\ldots\ldots\ldots\ldots \\ l_n &= \phantom{k_1 + k_2 + \ldots + {}} k_n. \end{aligned}$$

Il en résulte que

$$k_i = l_i - l_{i+1},\ k_n = l_n, \qquad i = 1, 2, \ldots, n-1,$$

c'est-à-dire on peut calculer les exposants $k_1, k_2, \ldots, k_n$ du terme initial du polynôme χ en fonction des exposants $l_1, l_2, \ldots, l_n$. Ainsi, les termes distincts du polynôme χ, en tant que polynômes de $x_1, x_2, \ldots, x_n$, ont les plus hauts termes *distincts*.

Considérons maintenant les termes du polynôme χ; calculons pour chaque terme de χ, représenté sous forme de polynôme de $x_1, x_2, \ldots, x_n$, son plus haut terme et fixons, parmi ces derniers, *le plus haut* terme dans le sens de l'ordre lexicographique. D'après la remarque faite ci-dessus, ce terme n'a pas de semblables parmi les plus hauts termes des autres monômes de χ exprimés en fonction des $x_1, x_2, \ldots, x_n$ et, étant supérieur au *plus haut* terme de chaque

monôme de χ, il est supérieur à tout autre terme exprimé en x_1, x_2, . . ., x_n au moyen des formules (1). Ainsi, nous avons trouvé un terme qui, à la suite du passage de $\chi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ à $g(x_1, x_2, \ldots, x_n)$, n'apparaît (avec un coefficient non nul) qu'une fois et, pour cette raison, ne peut pas disparaître. Il en résulte l'existence de coefficients non nuls dans l'expression du polynôme $g(x_1, x_2, \ldots, x_n)$, de sorte que g n'est pas l'élément nul de l'anneau $P[x_1, x_2, \ldots, x_n]$, ce qu'il fallait démontrer.

Le théorème que nous venons de démontrer peut être encore énoncé de la manière suivante:

Les polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_n$, *en tant qu'éléments de l'anneau des polynômes* $P[x_1, x_2, \ldots, x_n]$, *forment une famille algébriquement indépendante sur le champ P.*

§ 53*. Remarques complémentaires sur les polynômes symétriques

Remarques sur le théorème fondamental. La démonstration du théorème fondamental sur les polynômes symétriques, donnée au paragraphe précédent, permet de compléter l'énoncé de ce théorème par certains détails essentiels dont nous aurons besoin par la suite. D'abord, les coefficients du polynôme $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$, exprimant un polynôme symétrique donné $f(x_1, x_2, \ldots, x_n)$ en fonction des polynômes symétriques élémentaires, non seulement appartiennent au champ P, mais *s'expriment par les coefficients du polynôme f au moyen des opérations d'addition et de soustraction, c'est-à-dire qu'ils appartiennent à l'anneau L, engendré dans le champ P par les coefficients du polynôme f.*

En effet, les coefficients du polynôme φ_1 exprimé en fonction des indéterminées $x_1, x_2, \ldots, x_n$ (cf. formule (5) du paragraphe précédent) sont des multiples de coefficients entiers de a_0, coefficient du plus haut terme de f, et, par conséquent, appartiennent à l'anneau L. Supposons que les coefficients des polynômes $\varphi_1, \varphi_2, \ldots, \varphi_l$, exprimés en fonction des $x_1, x_2, \ldots, x_n$, soient des éléments de L. Alors, les coefficients du polynôme $f_l = f - \varphi_1 - \varphi_2 - \ldots - \varphi_l$ le sont aussi, de sorte que L contient les coefficients du polynôme φ_{l+1}, en tant que polynôme de $x_1, x_2, \ldots, x_n$.

D'autre part, *le degré du polynôme* $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ *par rapport à l'ensemble des indéterminées* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *est égal à celui du polynôme* $f(x_1, x_2, \ldots, x_n)$ *en chaque indéterminée* x_i. En effet, le terme (2) du paragraphe précédent étant le plus haut terme du polynôme f, l'entier k_1 est le degré de f en x_1, de sorte que, vu la symétrie de f, k_1 est le degré de f en chaque indéterminée x_i. Or, le degré de φ_1, par rapport à l'ensemble des indéterminées $\sigma_1, \sigma_2, \ldots, \sigma_n$, est, d'après (5) du paragraphe précédent, l'entier

$$(k_1 - k_2) + (k_2 - k_3) + \ldots + (k_{n-1} - k_n) + k_n = k_1.$$

Ensuite, le plus haut terme du polynôme f_1 étant inférieur à celui du polynôme f, le degré de f_1 en x_i ne dépasse pas le degré de f en chaque x_i. Or, le polynôme φ_2 tient le même rôle pour f_1 que φ_1 pour f, de sorte que le degré de φ_2 par rapport à l'ensemble des indéterminées σ est égal au degré de f_1 en chaque x_i, c'est-à-dire ce degré ne dépasse pas k_1, etc. Ainsi, le degré de $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ ne dépasse pas k_1. Vu qu'aucun φ_i avec $i > 1$ ne peut contenir les indéterminées $\sigma_1, \sigma_2, \ldots, \sigma_n$ élevées aux mêmes puissances que dans φ_1, le degré de $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ est exactement k_1. Cela démontre notre proposition.

Enfin, soit $a\sigma_1^{l_1} \sigma_2^{l_2} \ldots \sigma_n^{l_n}$ un des termes du polynôme $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$. L'entier

$$l_1 + 2l_2 + \ldots + nl_n$$

est dit *poids* de ce terme, c'est-à-dire le poids d'un terme est la somme des exposants multipliés par les indices des indéterminées correspondantes. Autrement dit, le poids d'un terme est son degré par rapport à l'ensemble des indéterminées $x_1, x_2, \ldots, x_n$, ce qui découle du théorème sur le degré du produit des polynômes (§ 51). La proposition suivante est vraie:

Si un polynôme symétrique homogène $f(x_1, x_2, \ldots, x_n)$ est de degré s par rapport à l'ensemble des indéterminées, alors tous les termes de son expression $\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n)$ par σ ont un même poids égal à s.

En effet, si le terme (2) du paragraphe précédent est le plus haut terme d'un polynôme homogène f, alors

$$s = k_1 + k_2 + \ldots + k_n.$$

Or, le poids du terme φ_1 est, d'après (5) du paragraphe précédent, l'entier

$$(k_1 - k_2) + 2(k_2 - k_3) + \ldots + (n-1)(k_{n-1} - k_n) + nk_n =$$
$$= k_1 + k_2 + k_3 + \ldots + k_n,$$

c'est-à-dire encore s. Ensuite, le polynôme $f_1 = f - \varphi_1$, en tant que différence de deux polynômes homogènes de degré s, est encore un polynôme homogène de degré s, de sorte que le terme φ_2 du polynôme φ est de poids s, etc.

Fractions rationnelles symétriques. Le théorème fondamental sur les polynômes symétriques peut être généralisé aux fractions rationnelles. Une fraction rationnelle $\frac{f}{g}$ de n indéterminées $x_1, x_2, \ldots, x_n$ est dite *symétrique* si elle est invariante par rapport à toute permutation des indéterminées. Il est facile de montrer que *cette définition ne dépend pas du choix du « représentant » de la fraction rationnelle, soit $\frac{f}{g}$ ou $\frac{f_0}{g_0}$.* En effet, soient ω une permutation des indéterminées et φ un polynôme des indéterminées $x_1, x_2, \ldots, x_n$. Convenons de

noter par φ^{ω} le polynôme qui s'obtient de φ après que les indéterminées subissent la permutation ω. D'après notre hypothèse, on a pour toute ω:

$$\frac{f}{g}=\frac{f^{\omega}}{g^{\omega}},$$

ou encore $fg^{\alpha}=gf^{\omega}$. D'autre part, de l'égalité

$$\frac{f}{g}=\frac{f_0}{g_0}$$

s'ensuit $fg_0=gf_0$, d'où $f^{\omega}g_0^{\omega}=g^{\omega}f_0^{\omega}$. Multipliant les deux membres de la dernière égalité par f, nous obtenons:

$$ff^{\omega}g_0^{\omega}=fg^{\omega}f_0^{\omega}=gf^{\omega}f_0^{\omega},$$

d'où, simplifiant par le facteur commun f^{ω}, on a $fg_0^{\omega}=gf_0^{\omega}$, ou encore

$$\frac{f_0^{\omega}}{g_0^{\omega}}=\frac{f}{g}=\frac{f_0}{g_0}.$$

Le *théorème* suivant est vrai:

Toute fraction rationnelle symétrique des indéterminées $x_1, x_2, \ldots, x_n$ à coefficients dans un champ P peut être représentée sous la forme d'une fraction rationnelle des polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_n$ à coefficients dans P.

En effet, soit une fraction rationnelle symétrique

$$\frac{f(x_1, x_2, \ldots, x_n)}{g(x_1, x_2, \ldots, x_n)}.$$

Supposant qu'elle soit simple, on pourrait démontrer que f et g sont des polynômes symétriques. Cependant, la méthode suivante est plus simple. Supposons que le polynôme g ne soit pas symétrique et multiplions le numérateur et le dénominateur de la fraction par le produit des $(n!-1)$ polynômes qui s'obtiennent de g par toutes les permutations des indéterminées, excepté la permutation identique. Ceci étant, il est facile de vérifier que le dénominateur est déjà un polynôme symétrique. La fraction étant symétrique, il en résulte que son numérateur l'est aussi; il suffit maintenant, afin de démontrer le théorème, d'exprimer le numérateur et le dénominateur de la fraction obtenue par les polynômes symétriques élémentaires.

Sommes des puissances. On rencontre souvent dans les applications des polynômes symétriques de la forme

$$s_k=x_1^k+x_2^k+\ldots+x_n^k, \qquad k=1, 2, \ldots,$$

c'est-à-dire la somme des puissances $k^{\text{èmes}}$ des indéterminées $x_1, x_2, \ldots, x_n$. Ces polynômes, appelés *sommes des puissances*, doivent s'exprimer, d'après le théorème fondamental, par les polynômes

symétriques élémentaires. Cependant, le calcul de ces expressions pour k grand est assez difficile; c'est pourquoi la relation que nous allons établir entre les polynômes s_1, s_2, ... et les polynômes σ_1, σ_2, ..., σ_n représente un grand intérêt.

D'abord, $s_1 = \sigma_1$. Ensuite, soit $k \leqslant n$; alors, il est facile de vérifier que

$$\left.\begin{array}{l} s_{k-1}\sigma_1 = s_k + S\,(x_1^{k-1}x_2)^{1}, \\ s_{k-2}\sigma_2 = S\,(x_1^{k-1}x_2) + S\,(x_1^{k-2}x_2x_3), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ s_{k-i}\sigma_i = S\,(x_1^{k-i+1}x_2\dots x_i) + S\,(x_1^{k-i}x_2\dots x_ix_{i+1}),\quad 2 \leqslant i \leqslant k-2, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ s_1\sigma_{k-1} = S\,(x_1^2x_2\dots x_{k-1}) + k\sigma_k. \end{array}\right\} \quad (1)$$

Formant la somme alternée de ces égalités (c'est-à-dire la somme des égalités (1) munies successivement des signes plus et moins) et faisant passer le second membre dans le premier, nous obtenons la formule suivante:

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0 \quad (k \leqslant n). \quad (2)$$

Pour $k > n$, les égalités (1) prennent la forme

$$\begin{array}{l} s_{k-1}\sigma_1 = s_k + S\,(x_1^{k-1}x_2), \\ s_{k-2}\sigma_2 = S\,(x_1^{k-1}x_2) + S\,(x_1^{k-2}x_2x_3), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ s_{k-i}\sigma_i = S\,(x_1^{k-i+1}x_2\dots x_i) + S\,(x_1^{k-i}x_2\dots x_ix_{i+1}),\qquad 2 \leqslant i \leqslant n-1, \\ \dots\dots\dots\dots\dots\dots \\ s_{k-n}\sigma_n = S\,(x_1^{k-n+1}x_2\dots x_n), \end{array}$$

d'où la formule

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 - \dots + (-1)^n s_{k-n}\sigma_n = 0 \qquad (k > n). \qquad (3)$$

Les formules (2) et (3) sont appelées *formules de Newton*. Elles établissent une relation entre les sommes des puissances et les polynômes symétriques élémentaires et permettent de trouver successivement les expressions des s_1, s_2, s_3, ... en fonction des σ_1, σ_2, ..., σ_n. Ainsi, on sait que $s_1 = \sigma_1$, ce qui découle également de la formule (2). Pour $k = 2 \leqslant n$, on a, d'après (2), $s_2 - s_1\sigma_1 + 2\sigma_2 = 0$, d'où

$$s_2 = \sigma_1^2 - 2\sigma_2.$$

[1] Cf. la formule (11) du paragraphe précédent.

Puis, pour $k=3\leqslant n$, on a : $s_3-s_2\sigma_1+s_1\sigma_2-3\sigma_3=0$, d'où, utilisant les expressions de s_1 et de s_2 déjà trouvées, on obtient :

$$s_3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3,$$

résultat connu du paragraphe précédent (cf. (12)). Pour $k = 3$, $n = 2$, on a, d'après (3), $s_3 - s_2\sigma_1 + s_1\sigma_2 = 0$, d'où $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2$. Utilisant les formules de Newton on peut établir la formule générale exprimant s_k en fonction des $\sigma_1, \sigma_2, \ldots, \sigma_n$. D'ailleurs, cette formule est assez encombrante et nous ne la donnerons pas.

Si le champ de base est de caractéristique nulle, de sorte que l'on peut diviser par tout nombre naturel n[1], alors la formule (2) donne un moyen d'exprimer successivement les polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_n$ par les n premières sommes des puissances, soit $s_1, s_2, \ldots, s_n$. Ainsi, $\sigma_1 = s_1$, de sorte que

$$\sigma_2=\frac{1}{2}(s_1\sigma_1-s_2)=\frac{1}{2}(s_1^2-s_2),$$

$$\sigma_3=\frac{1}{3}(s_3-s_2\sigma_1+s_1\sigma_2)=\frac{1}{6}(s_1^3-3s_1s_2+2s_3),$$

etc. De ce résultat et du théorème fondamental découle la proposition suivante :

Tout polynôme symétrique de n indéterminées $x_1, x_2, \ldots, x_n$ sur un champ P de caractéristique nulle peut être représenté sous la forme d'un polynôme des $s_1, s_2, \ldots, s_n$ à coefficients dans le champ P.

Polynômes symétriques par rapport à deux groupes d'indéterminées. Dans le paragraphe suivant, ainsi qu'au § 58, on utilisera une généralisation de la notion de polynôme symétrique. Soient deux groupes d'indéterminées $x_1, x_2, \ldots, x_n$ et $y_1, y_2, \ldots, y_r$; en outre, on suppose que les indéterminées

$$x_1, x_2, \ldots, x_n, \quad y_1, y_2, \ldots, y_r \tag{4}$$

soient algébriquement indépendantes sur un champ P. Un polynôme $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r)$ sur un champ P est dit *symétrique par rapport à deux groupes d'indéterminées* si f est invariant par rapport à toute permutation des indéterminées $x_1, x_2, \ldots, x_n$ et à toute permutation des indéterminées $y_1, y_2, \ldots, y_r$. Conservant les notations $\sigma_1, \sigma_2, \ldots, \sigma_n$ pour les polynômes symétriques élémentaires en $x_1, x_2, \ldots, x_n$ et introduisant les notations $\tau_1, \tau_2, \ldots, \tau_r$ pour les polynômes symétriques élémentaires en $y_1, y_2, \ldots, y_r$, le théorème fondamental se généralise de la manière suivante.

[1] Dans un champ de caractéristique p l'expression $\frac{a}{p}$ n'a pas de sens pour $a \neq 0$, car on a dans ce champ pour tout x : $px = 0$.

Tout polynôme $f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r)$ sur un champ P, symétrique par rapport à deux groupes d'indéterminées $x_1, x_2, \ldots, x_n$ et $y_1, y_2, \ldots, y_r$, peut être représenté sous la forme d'un polynôme (à coefficients dans P) des polynômes symétriques élémentaires $\sigma_1, \sigma_2, \ldots, \sigma_n$ et $\tau_1, \tau_2, \ldots, \tau_r$:

$$f(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r) = \\ = \varphi(\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r).$$

En effet, on peut considérer le polynôme f en tant que polynôme $\bar{f}(y_1, y_2, \ldots, y_r)$ à coefficients, polynômes de $x_1, x_2, \ldots, x_n$. f étant invariant par rapport aux permutations des indéterminées $x_1, x_2, \ldots, x_n$, les coefficients du polynôme $\bar{f}$ sont des polynômes symétriques en $x_1, x_2, \ldots, x_n$, de sorte que les coefficients de $\bar{f}$ peuvent être représentés, d'après le théorème fondamental, sous forme de polynômes (à coefficients dans P) de $\sigma_1, \sigma_2, \ldots, \sigma_n$. D'autre part, le polynôme $\bar{f}(y_1, y_2, \ldots, y_r)$, considéré sur le champ $P(x_1, x_2, \ldots, x_n)$, est symétrique en $y_1, y_2, \ldots, y_r$, de sorte que $\bar{f}$ peut être représenté sous la forme d'un polynôme de $\tau_1, \tau_2, \ldots, \tau_r$, soit $\bar{\varphi}(\tau_1, \tau_2, \ldots, \tau_r)$. Les coefficients du polynôme $\bar{\varphi}$ s'expriment par ceux du polynôme $\bar{f}$ au moyen de l'addition et de la soustraction (ceci a été montré au début de ce paragraphe), par conséquent, ils sont également des polynômes de $\sigma_1, \sigma_2, \ldots, \sigma_n$. Ceci conduit manifestement à l'expression cherchée de f en fonction des $\sigma_1, \sigma_2, \ldots, \sigma_n$ et $\tau_1, \tau_2, \ldots, \tau_r$.

Exemple. Le polynôme

$$f(x_1, x_2, x_3, y_1, y_2) = x_1x_2x_3 - x_1x_2y_1 - x_1x_2y_2 - \\ - x_1x_3y_1 - x_1x_3y_2 - x_2x_3y_1 - x_2x_3y_2 + x_1y_1y_2 + \\ + x_2y_1y_2 + x_3y_1y_2$$

est symétriqae par rapport aux indéterminées x_1, x_2, x_3 et y_1, y_2, mais il ne l'est pas par rapport à l'ensemble des cinq indéterminées; en effet, on peut faire apparaître ceci en transposant les indéterminées x_1 et y_1. Trouvons l'expression de f en fonction des $\sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2$:

$$f = x_1x_2x_3 - (x_1x_2 + x_1x_3 + x_2x_3)\, y_1 - \\ - (x_1x_2 + x_1x_3 + x_2x_3)\, y_2 + (x_1 + x_2 + x_3)\, y_1y_2 = \\ = \sigma_3 - \sigma_2 y_1 - \sigma_2 y_2 + \sigma_1 y_1 y_2 = \sigma_3 - \sigma_2\tau_1 + \sigma_1\tau_2.$$

Bien entendu, le théorème que nous venons de démontrer peut être généralisé au cas de trois et, généralement, de plusieurs groupes d'indéterminées.

Le *théorème d'unicité* de la représentation par les polynômes symétriques élémentaires est également vrai pour les polynômes symétriques par rapport à deux groupes d'indéterminées. Autrement dit, le *théorème* suivant est vrai.

La famille

$$\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r$$

des polynômes symétriques élémentaires dépendant respectivement d'un groupe d'indéterminées $x_1, x_2, \ldots, x_n$ *et d'un autre groupe d'indéterminées* $y_1, y_2, \ldots, y_r$ *est une famille algébriquement indépendante sur un champ* P.

En effet, supposons qu'il existe un polynôme sur un champ P

$$\varphi(\sigma_1, \sigma_2, \ldots, \sigma_n, \tau_1, \tau_2, \ldots, \tau_r),$$

égal à zéro, quoiqu'il possède des coefficients non nuls. Ce polynôme peut être considéré comme un polynôme $\psi(\tau_1, \tau_2, \ldots, \tau_r)$ à coefficients, polynômes de $\sigma_1, \sigma_2, \ldots, \sigma_n$. Donc, on peut dire que ψ est un polynôme de $\tau_1, \tau_2, \ldots, \tau_r$ sur le champ des fractions rationnelles

$$Q = P(x_1, x_2, \ldots, x_n).$$

La famille $y_1, y_2, \ldots, y_r$ reste algébriquement indépendante sur le champ Q: en effet, s'il existait une dépendance algébrique des $y_1, y_2, \ldots, y_r$ à coefficients dans Q, ceci entraînerait, après multiplication par le dénominateur commun, une dépendance algébrique de la famille (4), ce qui serait en contradiction avec notre hypothèse. En s'appuyant sur le théorème d'unicité démontré au paragraphe précédent, on voit que la famille $\tau_1, \tau_2, \ldots, \tau_r$ doit être aussi algébriquement indépendante sur le champ Q, de sorte que les coefficients du polynôme ψ sont tous nuls. Or, ces coefficients sont des polynômes de $\sigma_1, \sigma_2, \ldots, \sigma_n$; par conséquent, utilisant de nouveau le théorème d'unicité pour un groupe d'indéterminées (cette fois-ci par rapport aux indéterminées $x_1, x_2, \ldots, x_n$) nous constatons que les coefficients de ces derniers polynômes sont tous nuls. Ceci démontre que, contrairement à notre hypothèse, les coefficients du polynôme φ sont tous nuls.

§ 54*. Résultant. Elimination d'une indéterminée. Discriminant

Soit un polynôme $f(x_1, x_2, \ldots, x_n)$ de l'anneau $P[x_1, x_2, \ldots, x_n]$; une suite de n éléments $\alpha_1, \alpha_2, \ldots, \alpha_n$ du champ P ou d'une extension $\overline{P}$ est dite *solution* du polynôme f si les valeurs des indéterminées

$$x_1 = \alpha_1, \quad x_2 = \alpha_2, \quad \ldots, \quad x_n = \alpha_n$$

annulent le polynôme f:

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0.$$

Tout polynôme f de degré non nul possède des solutions. En effet, supposons que l'indéterminée x_1 intervienne dans l'expression de f et choisissons $\alpha_2, \ldots, \alpha_n$ dans le champ P de manière que le degré du polynôme $f(x_1, \alpha_2, \ldots, \alpha_n)$ soit strictement positif; utilisant,

ensuite, le théorème d'existence d'un zéro (cf. § 49), on peut trouver une extension $\bar{P}$ du champ P telle que le polynôme $f(x_1, \alpha_2, \ldots, \alpha_n)$ d'une indéterminée x_1 ait un zéro α_1 dans $\bar{P}$. En même temps, nous constatons que la propriété d'avoir au plus n zéros, établie pour les polynômes de degré n d'une indéterminée, n'est plus valable pour les polynômes de plusieurs indéterminées.

Soient plusieurs polynômes de n indéterminées; on peut poser le problème qui consiste à trouver les solutions communes à ces polynômes; autrement dit, on peut poser le problème de calcul des solutions du système d'équations ayant les polynômes donnés pour premiers membres et zéro pour seconds. Un cas particulier, celui des systèmes d'équations linéaires, a déjà été étudié en détail dans le chapitre II. Cependant, dans le cas particulier opposé, où l'on considère une équation d'une inconnue de degré quelconque, nous ne savons rien sur les racines, sauf qu'elles existent dans une certaine extension du champ de base. Le calcul et l'étude des solutions d'un système d'équations non linéaires à plusieurs inconnues est, évidemment, un problème encore plus difficile qui sort du cadre de notre cours et fait partie d'une branche spéciale des mathématiques, la géométrie algébrique. Nous nous bornerons ici à considérer *deux* équations de degrés quelconques à *deux* inconnues et montrerons que ce cas peut être ramené à celui *d'une* équation polynomiale à *une* inconnue.

Occupons-nous d'abord du problème d'existence des zéros communs aux deux polynômes dépendant d'une indéterminée. Soient deux polynômes

$$\left.\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \\ g(x) &= b_0x^s + b_1x^{s-1} + \ldots + b_{s-1}x + b_s \end{aligned}\right\} \quad (1)$$

sur un champ P, de plus $a_0 \neq 0$, $b_0 \neq 0$.

Des résultats du chapitre précédent il découle aisément que *les polynômes $f(x)$ et $g(x)$ ont des zéros communs dans une extension du champ P si et seulement si ils ne sont pas premiers entre eux.* Ainsi, le problème d'existence des zéros communs à deux polynômes peut être résolu au moyen de l'algorithme d'Euclide.

Nous allons indiquer une autre méthode permettant de résoudre ce problème. Soit $\bar{P}$ une extension du champ P telle que $f(x)$ ait exactement n zéros $\alpha_1, \alpha_2, \ldots, \alpha_n$ et que $g(x)$ possède exactement s zéros $\beta_1, \beta_2, \ldots, \beta_s$; on peut prendre pour $\bar{P}$ un champ de décomposition du produit $f(x)\,g(x)$. L'élément

$$R(f, g) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) \quad (2)$$

du champ $\overline{P}$ est dit *résultant* des deux polynômes $f(x)$ et $g(x)$. Il est clair que *$f(x)$ et $g(x)$ ont un zéro commun dans $\overline{P}$ si et seulement si $R(f, g) = 0$.* Vu que

$$g(x) = b_0 \prod_{j=1}^{s} (x - \beta_j)$$

et, par conséquent,

$$g(\alpha_i) = b_0 \prod_{j=1}^{s} (\alpha_i - \beta_j),$$

on constate que le résultant $R(f, g)$ peut être mis sous la forme

$$R(f, g) = a_0^s \prod_{i=1}^{n} g(\alpha_i). \tag{3}$$

Les polynômes $f(x)$ et $g(x)$ interviennent dans la définition du résultant de façon non symétrique. En effet,

$$R(g, f) = b_0^n a_0^s \prod_{j=1}^{s} \prod_{i=1}^{n} (\beta_j - \alpha_i) = (-1)^{ns} R(f, g). \tag{4}$$

$R(g, f)$, en accord avec (3), peut être mis sous la forme

$$R(g, f) = b_0^n \prod_{j=1}^{s} f(\beta_j). \tag{5}$$

L'expression (2) du résultant suppose la connaissance des zéros des polynômes $f(x)$ et $g(x)$ et, pour cette raison, est pratiquement inutile pour la résolution du probleme d'existence des zéros communs à ces polynômes. Il s'avère toutefois que *le résultant $R(f, g)$ peut être représenté sous la forme d'un polynôme des coefficients a_0, a_1, . . ., a_n et b_0, b_1, . . ., b_s de $f(x)$ et $g(x)$.*

La possibilité d'une telle représentation découle aisément des résultats du paragraphe précédent.

En effet, la formule (2) montre que le résultant $R(f, g)$ est un polynôme symétrique par rapport à deux groupes d'indéterminées, $\alpha_1, \alpha_2, \ldots, \alpha_n$ et $\beta_1, \beta_2, \ldots, \beta_s$. Par conséquent, en vertu des résultats du paragraphe précédent, il peut être représenté sous la forme d'un polynôme des polynômes symétriques élémentaires correspondant à ces deux groupes d'indéterminées, ou encore, vu les formules de Viète, sous la forme d'un polynôme des quotients $\frac{a_i}{a_0}$, $i = 1, 2, \ldots$ . . ., n, et $\frac{b_j}{b_0}$, $j = 1, 2, \ldots, s$; le facteur $a_0^s b_0^n$, inclus dans la formule (2), fait disparaître le dénominateur dans l'expression du résultant. Cependant il serait difficile de donner l'expression du résultant en fonction des coefficients à l'aide des méthodes exposées dans les paragraphes précédents; nous allons utiliser un autre procédé.

L'expression du résultant des polynômes (1) que nous allons trouver sera valable pour tout couple de polynômes. Plus ¡ récisé-

ment, *nous considérons la suite des zéros des polynômes* (1)

$$\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s \tag{6}$$

comme un ensemble de $n+s$ indéterminées indépendantes, c'est-à-dire un ensemble de $n+s$ éléments algébriquement indépendants sur le champ P au sens du § 51.

Nous trouverons une expression du résultant qui, considérée comme un polynôme des indéterminées (6) (les coefficients étant remplacés par les zéros d'après les formules de Viète), coïncide avec le second membre de l'égalité (2), considéré, lui aussi, comme un polynôme des indéterminées (6).

Nous montrerons que *le résultant $R(f, g)$ des polynômes* (1) *est égal au déterminant d'ordre $n+s$:*

$$D = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & & & \\ & a_0 & a_1 & \ldots & a_n & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & a_0 & a_1 & \ldots & a_n \\ b_0 & b_1 & \ldots & b_s & & & \\ & b_0 & b_1 & \ldots & b_s & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & b_0 & b_1 & \ldots & b_s \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} s \text{ lignes} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ lignes} \end{matrix} \tag{7}$$

l'égalité de $R(f, g)$ et du déterminant (7) étant identique par rapport à l'ensemble des indéterminées (6) (dans (7) les éléments non écrits sont des zéros). La structure de ce déterminant est assez simple; notons seulement que sa diagonale principale contient l'élément a_0 répété s fois et l'élément b_s répété n fois.

Afin de démontrer notre proposition nous calculerons de deux manières différentes le produit $a_0^s b_0^n DM$, où M est le déterminant auxiliaire d'ordre $n+s$:

$$M = \begin{vmatrix} \beta_1^{n+s-1} & \beta_2^{n+s-1} & \ldots & \beta_s^{n+s-1} & \alpha_1^{n+s-1} & \alpha_2^{n+s-1} & \ldots & \alpha_n^{n+s-1} \\ \beta_1^{n+s-2} & \beta_2^{n+s-2} & \ldots & \beta_s^{n+s-2} & \alpha_1^{n+s-2} & \alpha_2^{n+s-2} & \ldots & \alpha_n^{n+s-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \beta_1^2 & \beta_2^2 & \ldots & \beta_s^2 & \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \beta_1 & \beta_2 & \ldots & \beta_s & \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ 1 & 1 & \ldots & 1 & 1 & 1 & \ldots & 1 \end{vmatrix}.$$

M est un déterminant de Vandermonde et, d'après le § 6, il est égal au produit des différences des éléments de son avant-dernière ligne, les différences étant formées de la manière suivante: on retranche de chaque élément successivement les éléments qui le suivent.

Ainsi,

$$M = \prod_{1\leqslant i<j\leqslant s} (\beta_i-\beta_j)\cdot \prod_{j=1}^{s}\prod_{i=1}^{n} (\beta_j-\alpha_i)\cdot \prod_{1\leqslant i<j\leqslant n} (\alpha_i-\alpha_j),$$

de sorte que, vu (4), on a

$$a_0^s b_0^n DM = D\cdot R(g,\ f)\cdot \prod_{1\leqslant i<j\leqslant s} (\beta_i-\beta_j)\cdot \prod_{1\leqslant i<j\leqslant n} (\alpha_i-\alpha_j). \qquad (8)$$

D'autre part, calculons le produit DM utilisant le théorème sur le déterminant du produit de deux matrices. Multipliant les matrices, nous obtenons, vu que $\alpha_1, \alpha_2, \ldots, \alpha_n$ et $\beta_1, \beta_2, \ldots, \beta_s$ sont respectivement les zéros de $f(x)$ et de $g(x)$, la formule

$$DM = \begin{vmatrix} \beta_1^{s-1}f(\beta_1) & \beta_2^{s-1}f(\beta_2) & \ldots & \beta_s^{s-1}f(\beta_s) & 0 & 0 & \ldots & 0 \\ \beta_1^{s-2}f(\beta_1) & \beta_2^{s-2}f(\beta_2) & \ldots & \beta_s^{s-2}f(\beta_s) & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \beta_1 f(\beta_1) & \beta_2 f(\beta_2) & \ldots & \beta_s f(\beta_s) & 0 & 0 & \ldots & 0 \\ f(\beta_1) & f(\beta_2) & \ldots & f(\beta_s) & 0 & 0 & \ldots & 0 \\ 0 & 0 & & 0 & \alpha_1^{n-1}g(\alpha_1) & \alpha_2^{n-1}g(\alpha_2) & \ldots & \alpha_n^{n-1}g(\alpha_n) \\ 0 & 0 & & 0 & \alpha_1^{n-2}g(\alpha_1) & \alpha_2^{n-2}g(\alpha_2) & \ldots & \alpha_n^{n-2}g(\alpha_n) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & \alpha_1 g(\alpha_1) & \alpha_2 g(\alpha_2) & \ldots & \alpha_n g(\alpha_n) \\ 0 & 0 & \ldots & 0 & g(\alpha_1) & g(\alpha_2) & \ldots & g(\alpha_n) \end{vmatrix}.$$

Appliquant le théorème de Laplace, puis mettant en facteur les diviseurs communs des éléments d'une même colonne et calculant les déterminants correspondants (qui sont des déterminants de Vandermonde), nous obtenons l'égalité:

$$a_0^s b_0^n DM = a_0^s b_0^n \prod_{j=1}^{s} f(\beta_j)\cdot \prod_{1\leqslant i<j\leqslant s} (\beta_i-\beta_j)\cdot \prod_{i=1}^{n} g(\alpha_i)\cdot \prod_{1\leqslant i<j\leqslant n} (\alpha_i-\alpha_j)$$

ou encore, utilisant (3) et (5), la formule

$$a_0^s b_0^n DM = R(f,\ g)\, R(g,\ f)\cdot \prod_{1\leqslant i<j\leqslant s} (\beta_i-\beta_j)\cdot \prod_{1\leqslant i<j\leqslant n} (\alpha_i-\alpha_j). \qquad (9)$$

Nous obtenons que les seconds membres des égalités (8) et (9), en tant que polynômes des indéterminées (6), coïncident. Les deux membres de l'égalité obtenue peuvent être simplifiés en divisant par les facteurs communs non identiquement nuls. Le facteur commun $R(g,\ f)$ n'est pas nul: d'après notre hypothèse, $a_0 \neq 0$, $b_0 \neq 0$, et il suffit de donner aux indéterminées (6) des valeurs distinctes deux à deux (dans le champ de base ou dans une extension de ce

champ) pour obtenir, d'après la formule (4), une valeur non nulle du polynôme $R(g, f)$. On démontre de la même manière que les deux autres facteurs communs sont aussi non nuls. Divisant par les facteurs communs nous sommes conduits à l'égalité

$$R(f, g) = D, \tag{10}$$

ce qu'il fallait démontrer.

Renonçons à présent à la condition que les coefficients des termes principaux des polynômes (1) *doivent être non nuls* [1]. Donc, la seule chose qu'on puisse dire sur les degrés véritables des polynômes (1), c'est qu'ils ne dépassent pas respectivement n et s, degrés « formels » de $f(x)$ et de $g(x)$. L'expression (2) du résultant n'a plus de sens, car les polynômes considérés peuvent avoir respectivement moins de n et moins de s zéros. D'autre part, le déterminant (7) a toujours un sens et, vu que pour $a_0 \neq 0$, $b_0 \neq 0$ il coïncide avec le résultant, nous pouvons, dans le cas considéré, continuer à l'*appeler résultant* des polynômes $f(x)$, $g(x)$ et à le noter $R(f, g)$.

Toutefois, maintenant, on ne peut plus affirmer que l'existence des zéros communs aux polynômes (1) soit équivalente au fait que leur résultant s'annule. En effet, si $a_0 = 0$ et $b_0 = 0$, alors $R(f, g) = 0$ indépendamment de l'existence des zéros communs aux polynômes f et g. Néanmoins, il se révèle que ce cas est le seul où le résultant nul ne garantisse pas l'existence des zéros communs aux polynômes donnés [2]. Notamment, le théorème suivant est vrai :

Soient deux polynômes (1) *à coefficients des termes principaux quelconques; alors leur résultant* (7) *s'annule si et seulement si les polynômes* (1) *possèdent un zéro commun ou bien si les coefficients des termes principaux de ces polynômes s'annulent simultanément.*

Démonstration. Le cas où $a_0 \neq 0$, $b_0 \neq 0$ a déjà été considéré et le cas où $a_0 = b_0 = 0$ est prévu par l'énoncé du théorème. Il reste donc à considérer le cas où l'un des coefficients des termes principaux des polynômes (1), soit a_0, est non nul, tandis que l'autre coefficient b_0 est nul.

Si $b_i = 0$ pour tout i, $i = 0, 1, \ldots, s$, alors $R(f, g) = 0$, car le déterminant (7) a des lignes nulles. Mais alors le polynôme $g(x)$ est identiquement nul et, par conséquent, a des zéros communs avec $f(x)$. Supposons que

$$b_0 = b_1 = \ldots = b_{k-1} = 0, \quad \text{mais} \quad b_k \neq 0, \quad \text{avec } k \leqslant s;$$

[1] Nous renonçons à l'hypothèse sur le coefficient du terme principal, que nous avons jusqu'ici toujours imposée, ayant en vue les applications ultérieures : nous allons étudier les systèmes de polynômes de deux indéterminées en les considérant comme polynômes d'une indéterminée à coefficients, polynômes de l'autre. Par conséquent, le coefficient du terme principal peut s'annuler pour certaines valeurs de la seconde indéterminée.

[2] Bien entendu, le déterminant (7) est nul lorsque $a_n = b_s = 0$. Mais dans ce cas les polynômes (1) ont un zéro commun, à savoir 0.

soit

$$\bar{g}(x) = b_k x^{s-k} + b_{k+1} x^{s-k-1} + \ldots + b_{s-1} x + b_s ;$$

remplaçant dans le déterminant (7) les éléments $b_0, b_1, \ldots, b_{k-1}$ par des zéros et appliquant le théorème de Laplace, il vient:

$$R(f, g) = a_0^k R(f, \bar{g}). \tag{11}$$

Or, les coefficients des termes principaux des polynômes $f(x)$ et $\bar{g}(x)$ étant non nuls, l'égalité $R(f, \bar{g}) = 0$ est, en vertu du résultat obtenu ci-dessus, nécessaire et suffisante pour que f et $\bar{g}$ aient un zéro commun. D'autre part, les égalités $R(f, g) = 0$ et $R(f, \bar{g}) = 0$ étant, d'après (11), équivalentes et les polynômes g et $\bar{g}$ ayant manifestement les mêmes zéros, nous aboutissons au résultat cherché: dans le cas considéré l'égalité $R(f, g) = 0$ est équivalente à l'existence des zéros communs aux polynômes $f(x)$ et $g(x)$. Le théorème est démontré.

Calculons le résultant des polynômes quadratiques

$$f(x) = a_0 x^2 + a_1 x + a_2, \quad g(x) = b_0 x^2 + b_1 x + b_2.$$

D'après (7) on a

$$R(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix},$$

ou encore, développant le déterminant par rapport aux éléments de la première et de la troisième ligne, la formule

$$R(f, g) = (a_0 b_2 - a_2 b_0)^2 - (a_0 b_1 - a_1 b_0)(a_1 b_2 - a_2 b_1). \tag{12}$$

Ainsi, pour les polynômes

$$f(x) = x^2 - 6x + 2, \quad g(x) = x^2 + x + 5,$$

la formule (12) donne: $R(f, g) = 233$, de sorte que ces polynômes n'ont pas de zéros communs. Mais pour les polynômes

$$f(x) = x^2 - 4x - 5, \quad g(x) = x^2 - 7x + 10,$$

$R(f, g) = 0$; par conséquent, ces polynômes ont un zéro commun, à savoir le nombre 5.

Elimination d'une inconnue dans un système de deux équations à deux inconnues. Soient deux polynômes f et g à coefficients dans un champ P dépendant de deux indéterminées x et y. Ecrivons ces polynômes suivant les puissances décroissantes de x:

$$\left. \begin{aligned} f(x, y) &= a_0(y) x^k + a_1(y) x^{k-1} + \ldots + a_{k-1}(y) x + a_k(y), \\ g(x, y) &= b_0(y) x^l + b_1(y) x^{l-1} + \ldots + b_{l-1}(y) x + b_l(y); \end{aligned} \right\} \tag{13}$$

les coefficients sont des polynômes de l'anneau $P[y]$. Soit $R_x(f, g)$ le résultant des polynômes f et g, considérés comme des polynômes de x; d'après (7), $R_x(f, g)$ est un polynôme de y à coefficients dans le champ P:

$$R_x(f, g) = F(y). \tag{14}$$

Supposons que le système des polynômes (13) possède une solution commune, $x = \alpha$, $y = \beta$, dans une extension du champ P. Substituant dans (13) β à y, nous obtenons deux polynômes $f(x, \beta)$ et $g(x, \beta)$ de l'indéterminée x. Ces polynômes ont un zéro commun α, de sorte que leur résultant, qui, d'après (14), coïncide avec $F(\beta)$, doit s'annuler; autrement dit, β *doit être un zéro du résultant* $R_x(f, g)$. Inversement, si le résultant $R_x(f, g)$ des polynômes (13) a un zéro β, alors le résultant des polynômes $f(x, \beta)$ et $g(x, \beta)$ s'annule, c'est-à-dire *soit les polynômes* $f(x, \beta)$, $g(x, \beta)$ *ont un zéro commun, soit les coefficients de leurs termes principaux sont nuls,*

$$a_0(\beta) = b_0(\beta) = 0.$$

Ceci ramène le problème de calcul des solutions communes du système des polynômes (13) au problème de calcul des zéros du polynôme (14) dépendant d'une indéterminée y, ou encore, suivant la terminologie admise, *l'indéterminée x est éliminée, par ce procédé, du système des polynômes* (13).

Le théorème suivant permet de faire une conclusion sur le degré du polynôme qui s'obtient par l'élimination de l'une des indéterminées dans un système de deux polynômes de deux indéterminées:

Soient deux polynômes $f(x, y)$ et $g(x, y)$ respectivement de degrés n et s par rapport à l'ensemble des indéterminées x, y. Alors le degré du polynôme $R_x(f, g)$ en y n'est pas supérieur à ns, à condition, bien entendu, que $R_x(f, g)$ ne soit pas identiquement nul.

D'abord le résultant $R(f, g)$ de deux polynômes d'une indéterminée, dont les coefficients des termes principaux sont l'unité, est, d'après (2), un polynôme homogène de degré ns par rapport à $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_s$. Soit

$$a_1^{k_1} a_2^{k_2} \ldots a_n^{k_n} b_1^{l_1} b_2^{l_2} \ldots b_s^{l_s}$$

un terme de l'expression du résultant par les coefficients $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_s$; l'entier

$$k_1 + 2k_2 + \ldots + nk_n + l_1 + 2l_2 + \ldots + sl_s$$

est dit *poids* de ce terme. Il résulte de la remarque ci-dessus que *chaque terme dans l'expression de $R(f, g)$ par les coefficients a le même poids ns.* Ce résultat est encore vrai dans le cas général, à condition qu'on appelle *poids* d'un terme $a_0^{k_0} a_1^{k_1} \ldots a_n^{k_n} b_0^{l_0} b_1^{l_1} \ldots b_s^{l_s}$ l'entier

$$0 \cdot k_0 + 1 \cdot k_1 + \ldots + nk_n + 0 \cdot l_0 + 1 \cdot l_1 + \ldots + sl_s. \tag{15}$$

En effet, remplaçant dans le déterminant (7) les éléments a_0 et b_0 par l'unité, nous sommes ramenés au cas déjà considéré, mais les exposants de ces facteurs interviennent dans (15) avec le coefficient 0.

Ecrivons les polynômes f et g sous la forme:

$$f(x, y) = a_0(y) x^n + a_1(y) x^{n-1} + \ldots + a_n(y),$$
$$g(x, y) = b_0(y) x^s + b_1(y) x^{s-1} + \ldots + b_s(y).$$

Le degré de $f(x, y)$ par rapport à l'ensemble des indéterminées x, y étant n, le degré du coefficient $a_r(y)$, $r = 0, 1, \ldots, n$, n'est pas supérieur à son indice r; il en est de même pour $b_r(y)$. Il en résulte que le degré de chaque terme du résultant $R_x(f, g)$ n'est pas supérieur au poids de ce terme, c'est-à-dire au nombre ns, ce qu'il fallait démontrer.

Exemples.

1. Trouver les solutions communes du système des polynômes

$$f(x, y) = x^2y + 3xy + 2y + 3,$$
$$g(x, y) = 2xy - 2x + 2y + 3.$$

Eliminons l'indéterminée x; pour cela récrivons le système sous la forme

$$\left.\begin{aligned} f(x, y) &= y \cdot x^2 + (3y) \cdot x + (2y + 3), \\ g(x, y) &= (2y - 2) x + (2y + 3); \end{aligned}\right\} \qquad (16)$$

alors

$$R_x(f, g) = \begin{vmatrix} y & 3y & 2y+3 \\ 2y-2 & 2y+3 & 0 \\ 0 & 2y-2 & 2y+3 \end{vmatrix} = 2y^2 + 11y + 12.$$

Les zéros du résultant sont les nombres $\beta_1 = -4$, $\beta_2 = -\frac{3}{2}$. Ces valeurs de l'indéterminée y n'annulent pas les coefficients des termes principaux des polynômes (16); par conséquent, chacune de ces valeurs accouplée à une valeur correspondante de x fournit une solution du système des polynômes donnés. Les polynômes

$$f(x, -4) = -4x^2 - 12x - 5,$$
$$g(x, -4) = -10x - 5$$

ont un zéro commun $\alpha_1 = -\frac{1}{2}$. Les polynômes

$$f\left(x, -\frac{3}{2}\right) = -\frac{3}{2} x^2 - \frac{9}{2} x,$$
$$g\left(x, -\frac{3}{2}\right) = -5x$$

ont un zéro commun $\alpha_2 = 0$. Aussi, le système donné possède deux solutions:

$$\alpha_1 = -\frac{1}{2}, \ \beta_1 = -4 \ \text{et} \ \alpha_2 = 0, \ \beta_2 = -\frac{3}{2}.$$

2. Eliminer l'une des indéterminées dans le système des polynômes

$$f(x, y) = 2x^3y - xy^2 + x + 5,$$
$$g(x, y) = x^2y^2 + 2xy^2 - 5y + 1.$$

Les polynômes étant de deuxième degré en y et le premier polynôme du troisième degré en x, il est logique d'éliminer y. Récrivons le système sous

la forme

$$\left.\begin{array}{l} f(x, y) = (-x)\cdot y^2 + (2x^3)\cdot y + (x+5), \\ g(x, y) = (x^2+2x)\, y^2 - 5y + 1 \end{array}\right\} \qquad (17)$$

et calculons son résultant en appliquant la formule (12):

$$\begin{aligned} R_y(f, g) = &[(-x)\cdot 1 - (x+5)(x^2+2x)]^2 - \\ &-[(-x)(-5) - 2x^3(x^2+2x)][2x^3\cdot 1 - (x+5)(-5)] = \\ &= 4x^8 + 8x^7 + 11x^6 + 84x^5 + 161x^4 + 154x^3 + 96x^2 - 125x. \end{aligned}$$

L'un des zéros du résultant est 0. Or, cette valeur de l'indéterminée x annule les deux coefficients des termes principaux des polynômes (17); en outre, il est facile de vérifier que les polynômes $f(0, y)$ et $g(0, y)$ n'ont pas de zéros communs. Nous n'avons pas le moyen de calculer les autres zéros du résultant. On peut seulement affirmer que si nous pouvions les calculer (par exemple, dans un champ de décomposition de $R_y(f, g)$), aucun de ces zéros n'annulerait simultanément les deux coefficients des termes principaux des polynômes (17), de sorte que chacun des zéros du résultant $R_y(f, g)$ accouplé à une valeur (ou des valeurs) correspondante de y forme une solution du système des polynômes donnés.

Il existe des méthodes permettant d'éliminer successivement les indéterminées dans les systèmes composés d'un nombre quelconque de polynômes dépendant d'un nombre quelconque d'indéterminées. Ces méthodes trop laborieuses ne sauraient faire partie de notre cours.

Discriminant. Par analogie avec le problème qui nous a conduits à la notion de résultant, on peut parler des conditions d'existence des zéros multiples d'un polynôme $f(x)$ de degré n appartenant à l'anneau $P[x]$. Soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \qquad a_0 \neq 0,$$

et soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ les zéros de ce polynôme dans une extension du champ P. Il est clair que, *dans cette suite, il y a des zéros multiples si et seulement si le produit*

$$\begin{aligned} \Delta = &(\alpha_2-\alpha_1)(\alpha_3-\alpha_1)\ldots(\alpha_n-\alpha_1)\times \\ &\times(\alpha_3-\alpha_2)(\alpha_4-\alpha_2)\ldots(\alpha_n-\alpha_2)\times \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &\times(\alpha_n-\alpha_{n-1}) = \prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j) \end{aligned}$$

est égal à zéro ou encore si le produit

$$D = a_0^{2n-2}\prod_{n\geq i>j\geq 1}(\alpha_i-\alpha_j)^2,$$

dit *discriminant* du polynôme $f(x)$, *s'annule.*

Contrairement au produit Δ qui change de signe pour une transposition des zéros, le discriminant D est symétrique par rapport aux $\alpha_1, \alpha_2, \ldots, \alpha_n$ et, par conséquent, peut être exprimé en fonction des coefficients de $f(x)$. Pour trouver cette expression (*sous l'hypothèse que le champ de base P est de caractéristique nulle*) on peut se servir de la relation entre le discriminant d'un polynôme $f(x)$ et le résultant du polynôme $f(x)$ et de sa dérivée. Il est naturel de s'attendre à ce qu'une telle relation existe, car on sait du § 49 qu'un polynôme $f(x)$ possède des zéros multiples si et seulement si il a des zéros communs avec sa dérivée $f'(x)$; par conséquent, $D = 0$ si et seulement si $R(f, f') = 0$.

D'après la formule (3) de ce paragraphe on a

$$R(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

Dérivant l'égalité

$$f(x) = a_0 \prod_{k=1}^{n} (x - \alpha_k),$$

nous obtenons:

$$f'(x) = a_0 \sum_{k=1}^{n} \prod_{j \neq k} (x - \alpha_j).$$

Substituant α_i à x, tous les termes, excepté le $i^{\text{ème}}$, s'annulent, de sorte que

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

d'où l'on a

$$R(f, f') = a_0^{n-1} \cdot a_0^{n} \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Pour tout couple d'indices i et j, $i > j$, ce produit possède deux facteurs: $\alpha_i - \alpha_j$ et $\alpha_j - \alpha_i$. Leur produit est $(-1) \cdot (\alpha_i - \alpha_j)^2$; vu qu'il existe $\frac{n(n-1)}{2}$ couples d'indices i, j vérifiant les inégalités $n \geqslant i > j \geqslant 1$, on obtient

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0^{2n-1} \prod_{n \geqslant i > j \geqslant 1} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_0 D.$$

Exemple. Calculons le discriminant du trinôme du second degré

$$f(x) = ax^2 + bx + c.$$

Vu que $f'(x)=2ax+b$, on a

$$R(f, f')=\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix}=a(-b^2+4ac).$$

Dans notre cas $\frac{n(n-1)}{2}=1$ et l'on a

$$D=-a^{-1}R(f, f')=b^2-4ac.$$

Cette expression coïncide avec celle qu'il est admis d'appeler en algèbre élémentaire discriminant d'un trinôme du second degré.

Une autre méthode de calcul du discriminant consiste en ceci. Formons le déterminant de Vandermonde par rapport aux zéros $\alpha_1, \alpha_2, \ldots, \alpha_n$. D'après le § 6, on a

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{n\geqslant i>j\geqslant 1} (\alpha_i-\alpha_j)=\Delta,$$

de sorte que le discriminant est égal au carré de ce déterminant multiplié par a_0^{2n-2}. Multipliant ce déterminant par son transposé et appliquant le théorème sur le déterminant du produit de deux matrices, nous obtenons:

$$D=a_0^{2n-2}\begin{vmatrix} n & s_1 & s_2 & \ldots & s_{n-1} \\ s_1 & s_2 & s_3 & \ldots & s_n \\ s_2 & s_3 & s_4 & \ldots & s_{n+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{n-1} & s_n & s_{n+1} & \ldots & s_{2n-2} \end{vmatrix}, \qquad (18)$$

où s_k est la somme des puissances $k^{\text{èmes}}$ des zéros $\alpha_1, \alpha_2, \ldots, \alpha_n$, définie dans le paragraphe précédent.

Exemple. Calculons le discriminant du polynôme du troisième degré $f(x)=x^3+ax^2+bx+c$. D'après (18), on a

$$D=\begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}.$$

On sait du paragraphe précédent que

$$s_1=\sigma_1=-a,$$
$$s_2=\sigma_1^2-2\sigma_2=a^2-2b,$$
$$s_3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3=-a^3+3ab-3c.$$

Utilisant la formule de Newton et vu que $\sigma_4=0$, on trouve

$$s_4=\sigma_1^4-4\sigma_1^2\sigma_2+4\sigma_1\sigma_3+2\sigma_2^2=a^4-4a^2b+4ac+2b^2.$$

Il en résulte

$$D = 3s_2s_4 + 2s_1s_2s_3 - s_2^3 - s_1^2s_4 - 3s_3^2 = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2. \quad (19)$$

En particulier, pour $a = 0$, c'est-à-dire pour un polynôme du troisième degré non complet, on retrouve la formule

$$D = -4b^3 - 27c^2,$$

ce qui est en accord avec le résultat du § 38.

§ 55*. Seconde démonstration du théorème fondamental de l'algèbre des nombres complexes

La démonstration du théorème fondamental donnée au § 23 n'était pas algébrique. Nous voulons en donner une autre qui utilise essentiellement l'outil algébrique, notamment, le théorème fondamental sur les polynômes symétriques (§ 52), ainsi que le théorème d'existence d'un champ de décomposition pour tout polynôme (§ 49); en outre, la partie non algébrique de cette démonstration est réduite au minimum et n'utilise qu'une proposition analytique très simple.

Rappelons d'abord le lemme du module du terme principal démontré au § 23. Supposant les coefficients du polynôme $f(x)$ réels et faisant $k = 1$, nous obtenons de ce lemme le *corollaire* suivant:

Le signe d'un polynôme $f(x)$ à coefficients réels pour x réel et suffisamment grand en valeur absolue coïncide avec le signe de son terme principal.

Il en découle le résultat:

Tout polynôme de degré impair à coefficients réels possède au moins un zéro réel.

En effet, soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n,$$

où les coefficients a_i sont tous réels. n étant impair, le terme principal a_0x^n est de signes contraires pour x positif et négatif; par conséquent, vu le corollaire signalé ci-dessus, le polynôme $f(x)$ est de signes contraires pour x positif et négatif, suffisamment grand en valeur absolue. Il existe donc des valeurs de x, a et b, telles que

$$f(a) < 0, \qquad f(b) > 0.$$

Or, on sait du cours d'analyse qu'un polynôme $f(x)$ est une fonction continue et, en vertu de l'une des propriétés fondamentales des fonctions continues, il existe pour toute valeur c comprise entre $f(a)$ et $f(b)$ au moins une valeur x_0 de x, comprise entre a et b, telle que $f(x_0) = c$. En particulier, il existe un nombre α, compris entre a et b, tel que l'on ait: $f(\alpha) = 0$.

En nous appuyant sur ce résultat nous démontrerons la proposition suivante:

Tout polynôme de degré quelconque à coefficients réels possède au moins un zéro complexe.

En effet, soit un polynôme $f(x)$ à coefficients réels de degré $n = 2^k q$ avec q impair. Le cas $k = 0$ étant déjà considéré, nous supposons que $k > 0$, c'est-à-dire que n est pair. Nous allons raisonner par récurrence sur k, supposant que notre proposition soit déjà démontrée pour tout polynôme à coefficients réels, dont le degré est divisible par 2^{k-1} et non divisible par 2^k [1].

Soit P un champ de décomposition du polynôme $f(x)$ sur le champ des nombres complexes (cf. § 49) et soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ les zéros de $f(x)$, qui sont des éléments de P. Fixons un nombre réel, soit c, et formons les éléments du champ P

$$\beta_{ij} = \alpha_i\alpha_j + c(\alpha_i + \alpha_j), \qquad i < j. \tag{1}$$

Le nombre d'éléments β_{ij} est

$$\frac{n(n-1)}{2} = \frac{2^k q(2^k q-1)}{2} = 2^{k-1}q(2^k q-1) = 2^{k-1}q', \tag{2}$$

où q' est impair.

Formons maintenant un polynôme $g(x)$ de l'anneau $P[x]$ qui n'a d'autres zéros que les éléments β_{ij}, soit

$$g(x) = \prod_{i,\, j,\, i<j} (x - \beta_{ij}).$$

Les coefficients de $g(x)$ sont les polynômes symétriques élémentaires en β_{ij}. Par conséquent, ils sont, en vertu de (1), des polynômes de $\alpha_1, \alpha_2, \ldots, \alpha_n$ à coefficients réels (car c est réel); en outre, ces polynômes sont symétriques. En effet, la transposition de tout couple de zéros α_k et α_l n'entraîne qu'une transposition des β_{ij}: tout β_{kj} avec j différent de k et de l devient β_{lj} et inversement, tandis que β_{kl} et tous les β_{ij}, avec i, j différents de k et de l, sont conservés. Or, les coefficients du polynôme $g(x)$ ne varient pas par des permutations de ses zéros.

Il en résulte, d'après le théorème fondamental sur les polynômes symétriques, que les coefficients de $g(x)$ sont des polynômes (à coefficients réels) des coefficients du polynôme donné $f(x)$ et, par conséquent, les coefficients de $g(x)$ sont réels. Le degré de ce polynôme, égal au nombre de zéros β_{ij}, est, d'après (2), divisible par 2^{k-1} et n'est pas divisible par 2^k. Par conséquent, d'après l'hypothèse de récurrence, au moins l'un des zéros β_{ij} du polynôme $g(x)$ est un nombre complexe.

---

[1] Ce degré peut, par conséquent, être supérieur à n.

Ainsi, quel que soit le nombre réel c, on peut indiquer un couple d'indices i, j, avec $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, tel que l'élément $\alpha_i\alpha_j + c\,(\alpha_i + \alpha_j)$ soit un nombre complexe (rappelons que le champ P contient le champ des nombres complexes en tant que son sous-champ). Bien entendu, un autre choix du nombre c conduit à un autre couple d'indices correspondants. Or, les nombres réels forment un ensemble infini tandis qu'il n'y a qu'un nombre fini de couples d'indices i, j distincts. Il en résulte que l'on peut choisir deux nombres réels *distincts* c_1 et c_2 de manière qu'il leur corresponde *le même* couple d'indices i, j, pour lesquels les éléments

$$\left.\begin{aligned} \alpha_i\alpha_j + c_1(\alpha_i + \alpha_j) = a, \\ \alpha_i\alpha_j + c_2(\alpha_i + \alpha_j) = b \end{aligned}\right\} \tag{3}$$

sont des nombres complexes.

Les égalités (3) donnent

$$(c_1 - c_2)(\alpha_i + \alpha_j) = a - b,$$

d'où il s'ensuit :

$$\alpha_i + \alpha_j = \frac{a-b}{c_1 - c_2},$$

c'est-à-dire $\alpha_i + \alpha_j$ est un nombre complexe. Ce résultat et, par exemple, la première des égalités (3) donnent que le produit $\alpha_i\alpha_j$ est également un nombre complexe. Ainsi les éléments α_i et α_j sont les zéros du trinôme du second degré à coefficients complexes

$$x^2 - (\alpha_i + \alpha_j)\,x + \alpha_i\alpha_j = 0,$$

de sorte que α_i et α_j, en vertu de la formule du § 38 pour les zéros du trinôme du second degré à coefficients complexes, sont, eux aussi, des nombres complexes. Ainsi, nous avons trouvé parmi les zéros du polynôme $f(x)$ deux zéros qui sont des nombres complexes. Ceci démontre notre proposition.

Pour compléter la démonstration du théorème fondamental de l'algèbre il reste à considérer un polynôme à coefficients complexes. Soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

un tel polynôme. Soit un autre polynôme

$$\overline{f}(x) = \overline{a}_0x^n + \overline{a}_1x^{n-1} + \ldots + \overline{a}_n,$$

qui s'obtient de $f(x)$ en remplaçant ses coefficients par les nombres complexes conjugués ; considérons le produit :

$$F(x) = f(x)\,\overline{f}(x) = b_0x^{2n} + b_1x^{2n-1} + \ldots + b_kx^{2n-k} + \ldots + b_{2n},$$

avec

$$b_k = \sum_{i+j=k} a_i\overline{a}_j, \quad k = 0, 1, 2, \ldots, 2n.$$

Utilisant les propriétés des nombres complexes conjugués connues du § 18, nous obtenons

$$\overline{b}_k = \sum_{i+j=k} \overline{a}_i a_j = b_k,$$

c'est-à-dire les coefficients du polynôme $F(x)$ sont réels.

Alors, comme il a été démontré ci-dessus, $F(x)$ possède au moins un zéro complexe, soit β,

$$F(\beta) = f(\beta)\overline{f}(\beta) = 0,$$

c est-à-dire soit $f(\beta) = 0$, soit $\overline{f}(\beta) = 0$. Dans le premier cas le théorème est démontré. Si c'est le second cas qui a lieu, c'est-à-dire si

$$\overline{a}_0\beta^n + \overline{a}_1\beta^{n-1} + \ldots + \overline{a}_n = 0,$$

alors, remplaçant les nombres complexes intervenant dans cette égalité par leurs conjugués, nous obtenons:

$$f(\overline{\beta}) = a_0\overline{\beta}^n + a_1\overline{\beta}^{n-1} + \ldots + a_n = 0,$$

c'est-à-dire $f(x)$ a pour zéro le nombre complexe $\overline{\beta}$. La démonstration du théorème fondamental de l'algèbre est terminée.

Chapitre XII

POLYNÔMES À COEFFICIENTS RATIONNELS

§ 56*. Réductibilité des polynômes sur le champ des nombres rationnels

Aussi bien que les champs des nombres réels et complexes, le champ des nombres rationnels a pour nous un intérêt particulier; notons-le par R. C'est le plus petit des champs numériques: en effet, on a démontré au § 43 que le champ R appartient à tout champ numérique. C'est le problème de réductibilité des polynômes sur le champ des nombres rationnels qui nous intéresse à présent, tandis que le paragraphe suivant sera consacré aux zéros rationnels des polynômes à coefficients rationnels. Soulignons une fois de plus que ce sont deux problèmes différents; en effet, le polynôme

$$x^4+2x^2+1=(x^2+1)^2$$

est réductible sur le champ des nombres rationnels, bien qu'il n'ait pas de zéros rationnels.

Que peut-on dire de la réductibilité des polynômes sur le champ R? Faisons d'abord une remarque: soit un polynôme $f(x)$ dont les coefficients sont tous rationnels (mais pas forcément entiers); réduisant les coefficients au dénominateur commun et multipliant $f(x)$ par ce dénominateur k, nous obtenons le polynôme $kf(x)$ dont les coefficients sont tous des nombres entiers. Il est clair que les polynômes $f(x)$ et $kf(x)$ ont les mêmes zéros; d'autre part, ils sont simultanément réductibles ou irréductibles sur le champ R.

Cependant, nous n'avons pas acquis pour le moment le droit de considérer seuls des polynômes à coefficients entiers. En effet, soit un polynôme à coefficients entiers $g(x)$ réductible sur le champ des nombres rationnels, c'est-à-dire $g(x)$ se décompose en facteurs à coefficients rationnels de degrés inférieurs (dans le cas général, les coefficients des facteurs sont fractionnaires). Peut-on en déduire que $g(x)$ se décompose en facteurs à coefficients entiers? Autrement dit, est-il possible qu'un polynôme à coefficients entiers soit réductible sur le champ des nombres rationnels, mais irréductible sur l'anneau des nombres entiers?

La solution de ces problèmes peut être obtenue au moyen de raisonnements analogues à ceux donnés au § 51. Un polynôme $f(x)$ à coefficients entiers est dit *primitif* si ses coefficients sont premiers

entre eux, c'est-à-dire s'ils n'ont d'autres diviseurs communs que 1 et —1. Soit un polynôme $\varphi(x)$ à coefficients rationnels; alors $\varphi(x)$ peut être représenté de façon unique sous la forme d'un produit d'une fraction irréductible et d'un polynôme primitif:

$$\varphi(x) = \frac{a}{b} f(x); \tag{1}$$

pour cela il faut mettre en facteur le dénominateur commun des coefficients du polynôme $\varphi(x)$, puis les facteurs communs des numérateurs des coefficients; notons que le degré de $f(x)$ est égal à celui de $\varphi(x)$. L'unicité de la représentation (1) (au signe près) se démontre de la manière suivante. Soit

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x),$$

où $g(x)$ est encore un polynôme primitif. Alors

$$adf(x) = bcg(x).$$

Ainsi, ad et bc sont obtenus en mettant en facteur les diviseurs communs des coefficients entiers d'un même polynôme. Par conséquent, ils coïncident au signe près. Il en résulte que les polynômes primitifs $f(x)$ et $g(x)$ coïncident également au signe près.

Pour les polynômes primitifs à coefficients entiers le *lemme de Gauss* est vrai:

Le produit de deux polynômes primitifs est un polynôme primitif.

En effet, soient deux polynômes primitifs

$$f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_ix^{k-i} + \ldots + a_k,$$
$$g(x) = b_0x^l + b_1x^{l-1} + \ldots + b_jx^{l-j} + \ldots + b_l$$

et soit

$$f(x)g(x) = c_0x^{k+l} + c_1x^{k+l-1} + \ldots + c_{i+j}x^{(k+l)-(i+j)} + \ldots + c_{k+l}.$$

Supposant que ce produit ne soit pas primitif, il existe un nombre *premier* p tel qu'il soit un diviseur de tous les coefficients $c_0, c_1, \ldots$ $\ldots, c_{k+l}$. Les coefficients du polynôme primitif $f(x)$ n'étant pas tous divisibles par p, soit a_i le premier coefficient de $f(x)$ n'ayant pas p pour diviseur; de même, désignons par b_j le premier coefficient du polynôme $g(x)$ qui ne soit pas divisible par p. Multipliant terme à terme $f(x)$ et $g(x)$ et groupant les termes contenant $x^{(k+l)-(i+j)}$, il vient:

$$c_{i+j} = a_ib_j + a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \ldots + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \ldots$$

Le premier membre de cette égalité est divisible par p. Il en est de même pour tous les termes du second membre, excepté le premier; en effet, vu les conditions imposées sur le choix de i et j, les coeffi-

cients a_{i-1}, a_{i-2}, ... et b_{j-1}, b_{j-2}, ... sont tous divisibles par p. Il en résulte que le produit $a_i b_j$ est également divisible par p, de sorte que, p étant un nombre premier, au moins un des coefficients a_i, b_j doit être divisible par p, ce qui, toutefois, n'a pas lieu. La démonstration du lemme est terminée.

Passons à la résolution des problèmes posés ci-dessus. Supposons qu'un polynôme $g(x)$ de degré n à coefficients entiers soit réductible sur le champ des nombres rationnels:

$$g(x) = \varphi_1(x)\,\varphi_2(x),$$

$\varphi_1(x)$ et $\varphi_2(x)$ étant des polynômes à coefficients rationnels de degrés inférieurs à n. Alors

$$\varphi_i(x) = \frac{a_i}{b_i} f_i(x), \qquad i = 1, 2,$$

où $\frac{a_i}{b_i}$ est une fraction irréductible et $f_i(x)$ un polynôme primitif. On en déduit

$$g(x) = \frac{a_1 a_2}{b_1 b_2}\,[f_1(x)\,f_2(x)].$$

Le premier membre de cette égalité est un polynôme à coefficients entiers, de sorte que l'on peut simplifier le second membre en divisant par $b_1 b_2$. Or, le polynôme entre crochets, en vertu du lemme de Gauss, est primitif et, par conséquent, tout facteur premier du produit $b_1 b_2$ doit être, en même temps, un facteur du produit $a_1 a_2$; a_i et b_i étant premiers entre eux, $i = 1, 2$, le nombre a_2 doit être divisible par b_1 et le nombre a_1 par b_2:

$$a_2 = b_1 a_2', \quad a_1 = b_2 a_1'.$$

Il en résulte

$$g(x) = a_1' a_2' f_1(x)\,f_2(x).$$

Groupant le coefficient $a_1' a_2'$ avec un des facteurs $f_1(x)$, $f_2(x)$, nous obtenons une décomposition du polynôme $g(x)$ en facteurs à coefficients entiers de degrés inférieurs. Ceci démontre le *théorème* suivant :

Un polynôme à coefficients entiers irréductible sur l'anneau des nombres entiers l'est aussi sur le champ des nombres rationnels.

Nous sommes maintenant en droit de nous limiter, en examinant tels ou tels problèmes de la réductibilité des polynômes sur le champ des nombres rationnels, à la considération des décompositions des polynômes à coefficients entiers en facteurs dont tous les coefficients sont également des nombres entiers.

On sait déjà que tout polynôme de degré supérieur au premier est réductible sur le champ des nombres complexes et que tout polynôme à coefficients réels de degré supérieur au deuxième l'est sur le champ des nombres réels. La situation est tout autre dans le cas du champ des nombres rationnels: *pour tout entier positif n on peut*

indiquer un polynôme à coefficients rationnels (même entiers) de degré n tel qu'il soit irréductible sur le champ des nombres rationnels. La démonstration de cette proposition est basée sur une condition suffisante d'irréductibilité des polynômes sur le champ R, dite *critère d'Eisenstein*:

Soit un polynôme à coefficients entiers

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Supposons qu'il existe au moins un nombre premier p vérifiant les conditions suivantes:

1) *le coefficient principal a_0 de $f(x)$ n'est pas divisible par p,*
2) *les autres coefficients sont divisibles par p,*
3) *le terme indépendant de x se divisant par p n'est pas divisible par p^2;*

alors le polynôme $f(x)$ est irréductible sur le champ des nombres rationnels.

En effet, si le polynôme $f(x)$ est réductible sur le champ R, alors il se décompose en un produit de deux facteurs à coefficients entiers de degrés inférieurs:

$$f(x) = (b_0x^k + b_1x^{k-1} + \ldots + b_k)(c_0x^l + c_1x^{l-1} + \ldots + c_l),$$

où $k < n$, $l < n$, $k + l = n$. Identifiant les coefficients des mêmes puissances de x dans les deux membres de cette égalité, on en déduit:

$$\left.\begin{array}{l} a_n = b_kc_l, \\ a_{n-1} = b_kc_{l-1} + b_{k-1}c_l, \\ a_{n-2} = b_kc_{l-2} + b_{k-1}c_{l-1} + b_{k-2}c_l, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_0 = b_0c_0. \end{array}\right\} \qquad (2)$$

a_n étant divisible par p et p étant un nombre premier, la première des égalités (2) donne qu'au moins un des facteurs b_k, c_l est divisible par p. Ils ne peuvent pas être divisibles par p tous les deux, car, d'après notre hypothèse, a_n n'est pas divisible par p^2. Supposons, par exemple, que b_k soit divisible par p, alors c_l et p sont premiers entre eux. Passons à la seconde égalité (2). Son premier membre ainsi que le premier terme du second membre sont divisibles par p, de sorte que le produit $b_{k-1}c_l$ l'est aussi; c_l n'étant pas divisible par p, b_{k-1} doit avoir p pour facteur. De la même manière, nous déduisons de la troisième égalité (2) que b_{k-2} est divisible par p, etc. Enfin, nous obtenons de la $(k + 1)^{\text{ème}}$ égalité que b_0 est divisible par p; or, la dernière égalité (2) permet alors d'affirmer que a_0 est aussi divisible par p, ce qui est en contradiction avec notre hypothèse.

Il est très facile d'indiquer pour tout n des polynômes à coefficients entiers de degré n vérifiant les conditions du critère d'Eisenstein ; par conséquent, ces polynômes sont irréductibles sur le champ des nombres rationnels. Tel est, par exemple, le polynôme $x^n + 2$; on peut appliquer à ce polynôme le critère d'Eisenstein avec $p = 2$.

Le critère d'Eisenstein n'est qu'une condition suffisante d'irréductibilité sur le champ R et non nécessaire, c'est-à-dire si pour un polynôme $f(x)$ on ne peut pas trouver un nombre premier p vérifiant les conditions du critère d'Eisenstein, ce polynôme peut être aussi bien réductible, comme l'est, par exemple, $x^2 - 5x + 6$, qu'irréductible, comme l'est, par exemple, $x^2 + 1$. Outre le critère d'Eisenstein il existe bien d'autres critères moins importants d'irréductibilité des polynômes sur le champ R. Il existe aussi une méthode due à Kronecker, permettant de dire pour tout polynôme à coefficients entiers s'il est réductible ou irréductible sur le champ R. Cependant, cette méthode est trop laborieuse et pratiquement inapplicable.

Exemple. Considérons le polynôme

$$f_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

où p est un nombre premier. Les zéros de ce polynôme sont les valeurs de la racine $p^{\text{ème}}$ de l'unité, excepté la valeur 1 ; les valeurs de la racine $p^{\text{ème}}$ de l'unité divisant la circonférence de rayon unité du plan complexe en p arcs de longueur égale, le polynôme $f_p(x)$ est dit *polynôme de subdivision de la circonférence*.

Nous ne pouvons pas appliquer directement à ce polynôme le critère d'Eisenstein. Effectuons toutefois un changement d'indéterminée en posant $x = y + 1$. Nous obtenons:

$$g(y) = f_p(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} = \frac{1}{y}\left[y^p + py^{p-1} + \frac{p(p-1)}{2!}y^{p-2} + \ldots + py\right] =$$
$$= y^{p-1} + py^{p-2} + \frac{p(p-1)}{2!}y^{p-3} + \ldots + p.$$

Les coefficients du polynôme $g(y)$ coïncidant avec ceux du binôme de Newton, tous ces coefficients, excepté le coefficient du terme principal, sont divisibles par p ; en outre, le terme indépendant de y n'est pas divisible par p^2. Ainsi, d'après le critère d'Eisenstein, le polynôme $g(y)$ est irréductible sur le champ R. Il en découle *l'irréductibilité du polynôme de subdivision de la circonférence $f_p(x)$ sur le champ R*. En effet, supposant que

$$f_p(x) = \varphi(x)\psi(x),$$

on aurait

$$g(y) = \varphi(y+1)\psi(y+1).$$

§ 57*. Zéros rationnels des polynômes à coefficients entiers

On a indiqué ci-dessus que le problème de la décomposition d'un polynôme donné sur le champ des nombres rationnels en facteurs irréductibles n'a pratiquement pas de solution satisfaisante. Néan-

moins, un cas particulier de ce problème ayant trait à la séparation des facteurs linéaires d'un polynôme à coefficients rationnels, c'est-à-dire le problème de calcul des zéros rationnels de ce polynôme, est déjà assez simple et ne nécessite pas de calculs laborieux. Bien entendu le problème de calcul des zéros rationnels des polynômes à coefficients rationnels n'épuise aucunement le problème de calcul des zéros réels de ces polynômes, de sorte que les méthodes et résultats exposés dans le chapitre IX conservent entièrement leur importance pour les polynômes à coefficients rationnels.

Abordant le problème de calcul des zéros rationnels d'un polynôme à coefficients rationnels notons que, d'après la remarque du paragraphe précédent, on peut se borner à la considération des polynômes à coefficients entiers; en outre, nous considérerons séparément le cas de zéros entiers et celui de zéros fractionnaires.

Supposons qu'un nombre entier α *soit un zéro d'un polynôme* $f(x)$ *à coefficients entiers*; *alors* α *est un diviseur du terme indépendant de* x *de ce polynôme.*

En effet, soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n.$$

Divisons $f(x)$ par $x-\alpha$:

$$f(x) = (x-\alpha)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}).$$

Effectuant la division par la méthode de Hörner exposée au § 22, nous obtenons que *les coefficients du quotient, y compris* b_{n-1}, *sont des nombres entiers*; vu que

$$a_n = -\alpha b_{n-1} = \alpha(-b_{n-1}),$$

notre proposition en résulte[1].

Ainsi, si un polynôme à coefficients entiers $f(x)$ possède des zéros entiers, alors ces zéros se trouvent parmi les diviseurs du terme indépendant de x de $f(x)$. Il faut donc essayer successivement tous les diviseurs du terme indépendant de x, aussi bien positifs que négatifs; si aucun de ces diviseurs n'est zéro du polynôme, cela signifie que $f(x)$ ne possède pas de zéros entiers.

L'essai de tous les diviseurs du terme indépendant de x peut s'avérer assez laborieux même si l'on calcule les valeurs correspondantes du polynôme par la méthode de Hörner et non en remplaçant successivement l'indéterminée par les diviseurs en question. Les remarques qui suivent permettent de simplifier un peu les calculs.

---

[1] Il serait erroné d'essayer de démontrer ce théorème en se référant à ce que le terme indépendant de x a_n est (au signe près) le produit des zéros du polynôme $f(x)$, car parmi ces zéros peuvent se trouver des nombres fractionnaires, irrationnels et complexes, de sorte qu'on ne peut pas affirmer a priori que le produit de tous les zéros, excepté α, soit un nombre entier.

Tout d'abord, 1 et -1 étant toujours des diviseurs du terme indépendant de x, commençons par calculer $f(1)$ et $f(-1)$, ce qui ne représente pas de difficulté. Ensuite, soit α un zéro entier de $f(x)$; alors

$$f(x)=(x-\alpha)\,q(x),$$

où, comme il a été indiqué ci-dessus, les coefficients du quotient $q(x)$ sont tous des entiers, de sorte que les quotients

$$\frac{f(1)}{\alpha-1}=-q(1), \qquad \frac{f(-1)}{\alpha+1}=-q(-1)$$

doivent être des nombres entiers. Ainsi, *on ne doit essayer que tout diviseur, soit* α, *pour lequel les quotients* $\frac{f(1)}{\alpha-1}$, $\frac{f(-1)}{\alpha+1}$ *sont des nombres entiers* (α étant différent de 1 et -1).

Exemples. 1. Calculer les zéros entiers du polynôme

$$f(x)=x^3-2x^2-x-6.$$

Les diviseurs du terme indépendant de x sont les nombres ± 1, ± 2, ± 3, ± 6. Vu que $f(1)=-8$, $f(-1)=-8$, les nombres 1 et -1 ne sont pas des zéros de $f(x)$. Ensuite, les nombres

$$\frac{-8}{2+1},\quad \frac{-8}{-2-1},\quad \frac{-8}{6-1},\quad \frac{-8}{-6-1}$$

étant fractionnaires, les diviseurs 2, -2, 6, -6 doivent être éliminés, tandis que, les nombres

$$\frac{-8}{3-1},\quad \frac{-8}{3+1},\quad \frac{-8}{-3-1},\quad \frac{-8}{-3+1}$$

étant entiers, les diviseurs 3 et -3 sont à essayer. Appliquons la méthode de Hörner :

$$\begin{array}{r|rrrr} & 1 & -2 & -1 & -6 \\ \hline -3 & 1 & -5 & 14 & -48 \end{array},$$

c'est-à-dire $f(-3)=-48$ et le nombre -3 n'est pas un zéro de $f(x)$. Enfin

$$\begin{array}{r|rrrr} & 1 & -2 & -1 & -6 \\ \hline 3 & 1 & 1 & 2 & 0 \end{array},$$

c'est-à-dire $f(3)=0$ et le nombre 3 est un zéro de $f(x)$. En même temps, nous avons trouvé les coefficients du quotient de la division de $f(x)$ par $x-3$:

$$f(x)=(x-3)(x^2+x+2).$$

Il est facile de voir que le quotient x^2+x+2 n'a pas le nombre 3 pour zéro, c'est-à-dire ce nombre n'est pas un zéro multiple de $f(x)$.

2. Calculer les zéros entiers du polynôme

$$f(x)=3x^4+x^3-5x^2-2x+2.$$

Ici les diviseurs du terme indépendant de x sont ± 1 et ± 2. Ensuite, $f(1) = -1$, $f(-1) = 1$, c'est-à-dire 1 et -1 ne sont pas des zéros de $f(x)$. Enfin, les nombres

$$\frac{1}{2+1} \quad \text{et} \quad \frac{-1}{-2-1}$$

étant fractionnaires, les nombres 2 et -2 ne sont pas des zéros de $f(x)$; par conséquent, $f(x)$ n'a pas de zéros entiers.

Passons au problème de calcul des zéros fractionnaires.

Soit un polynôme à coefficients entiers; supposons de plus que le coefficient du terme principal de ce polynôme soit égal à l'unité. Alors tout zéro rationnel de ce polynôme est un nombre entier.

En effet, soit un polynôme à coefficients entiers

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n$$

et soit une fraction irréductible $\frac{b}{c}$, zéro de $f(x)$, c'est-à-dire on a

$$\frac{b^n}{c^n} + a_1 \frac{b^{n-1}}{c^{n-1}} + a_2 \frac{b^{n-2}}{c^{n-2}} + \ldots + a_n = 0.$$

On en déduit

$$\frac{b^n}{c} = -a_1 b^{n-1} - a_2 b^{n-2} c - \ldots - a_n c^{n-1},$$

c'est-à-dire une fraction irréductible est égale à un nombre entier, ce qui est impossible.

Le problème de calcul des zéros rationnels (fractionnaires et entiers) d'un polynôme à coefficients entiers

$$f(x) = a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_{n-1} x + a_n$$

est équivalent au problème de calcul des zéros entiers du polynôme

$$\varphi(y) = y^n + a_1 y^{n-1} + a_0 a_2 y^{n-2} + \ldots + a_0^{n-2} a_{n-1} y + a_0^{n-1} a_n,$$

notamment, pour trouver les zéros de $f(x)$ il faut diviser ceux de $\varphi(y)$ par a_0.

En effet, multiplions $f(x)$ par a_0^{n-1} et effectuons ensuite un changement d'indéterminée, en posant $y = a_0 x$. Il est clair que

$$\varphi(y) = \varphi(a_0 x) = a_0^{n-1} f(x).$$

Il en résulte que les zéros du polynôme $f(x)$ coïncident avec les zéros correspondants de $\varphi(y)$ divisés par a_0. En particulier, aux zéros rationnels de $f(x)$ correspondent les zéros rationnels de $\varphi(y)$; mais, étant donné que le coefficient du terme principal de $\varphi(y)$ est égal à l'unité, les zéros rationnels de $\varphi(y)$ doivent être entiers, et nous avons déjà une méthode de leur calcul.

Exemple. Trouver les zéros rationnels du polynôme

$$f(x) = 3x^4 + 5x^3 + x^2 + 5x - 2.$$

Multipliant $f(x)$ par 3^3 et faisant $y = 3x$, il vient :

$$\varphi(y) = y^4 + 5y^3 + 3y^2 + 45y - 54.$$

Calculons les zéros entiers du polynôme $\varphi(y)$.

Calculons $\varphi(1)$ par la méthode de Hörner :

$$1 \left| \begin{array}{ccccc} 1 & 5 & 3 & 45 & -54 \\ \hline 1 & 6 & 9 & 54 & 0 \end{array} \right. .$$

Ainsi $\varphi(1) = 0$, c'est-à-dire 1 est un zéro de $\varphi(y)$; en outre,

$$\varphi(y) = (y-1)\, q(y),$$

où

$$q(y) = y^3 + 6y^2 + 9y + 54.$$

Calculons les zéros entiers du polynôme $q(y)$. Les diviseurs du terme indépendant de y sont : ± 1, ± 2, ± 3, ± 6, ± 9, ± 18, ± 27, ± 54. Ici

$$q(1) = 70, \quad q(-1) = 50.$$

Calculant $\frac{q(1)}{\alpha - 1}$ et $\frac{q(-1)}{\alpha + 1}$ pour chaque diviseur α, on constate que l'on doit éliminer tous les diviseurs, excepté $\alpha = -6$. Essayons ce diviseur :

$$-6 \left| \begin{array}{cccc} 1 & 6 & 9 & 54 \\ \hline 1 & 0 & 9 & 0 \end{array} \right. .$$

Ainsi, $q(-6) = 0$, c'est-à-dire -6 est un zéro de $q(y)$ et, par conséquent, de $\varphi(y)$.

Le polynôme $\varphi(y)$ possède donc deux zéros entiers 1 et -6. Par conséquent, le polynôme $f(x)$ n'a que deux zéros rationnels, soit les nombres $\frac{1}{3}$ et -2.

On doit souligner une fois de plus que les méthodes exposées ci-dessus ne peuvent être appliquées qu'aux polynômes à coefficients entiers et uniquement pour calculer les zéros rationnels de ces polynômes.

§ 58*. Nombres algébriques

Tout polynôme de degré n à coefficients rationnels possède dans le champ des nombres complexes n zéros ; certains zéros (tous quelquefois) n'appartiennent pas au champ des nombres rationnels. Par contre, ce n'est pas tout nombre complexe ou réel qui est un zéro d'un polynôme à coefficients rationnels. Les nombres complexes (et, en particulier, les nombres réels) qui sont zéros de tels polynômes sont appelés nombres *algébriques*, contrairement aux nombres *transcendants*. L'ensemble des nombres algébriques contient les nombres rationnels, en tant que zéros des polynômes du premier degré à coefficients rationnels, ainsi que les nombres de la forme $\sqrt[n]{a}$ avec a ration-

nel, en tant que zéros des binômes $x^n - a$. D'autre part, on démontre dans les cours d'analyse que le nombre e, base des logarithmes de Neper, ainsi que le nombre π, bien connu de la géométrie élémentaire, sont des nombres transcendants.

Si α est un nombre algébrique, alors α est zéro d'un polynôme à coefficients entiers et, par conséquent, zéro d'un des facteurs irréductibles à coefficients entiers de ce polynôme. *Le polynôme irréductible à coefficients entiers ayant α pour zéro est bien défini à un facteur constant près, c'est-à-dire il est unique à condition que ses coefficients soient premiers entre eux* (c'est-à-dire à condition que ce polynôme soit primitif). En effet, si α est zéro de deux polynômes irréductibles $f(x)$ et $g(x)$, le plus grand commun diviseur de ces polynômes est différent de l'unité, de sorte que ces polynômes, étant irréductibles, coïncident à un facteur de degré nul près.

Les nombres algébriques qui sont zéros d'un même polynôme irréductible (sur le champ R) sont dits *conjugués* [1]. Par conséquent, l'ensemble des nombres algébriques est une réunion des classes disjointes finies de nombres algébriques conjugués. Un nombre rationnel, en tant que zéro d'un polynôme du premier degré, n'a pas de nombres algébriques conjugués, excepté lui-même; d'ailleurs, cette propriété est caractéristique pour les nombres rationnels, car tout nombre algébrique non rationnel est zéro d'un polynôme irréductible dont le degré est supérieur au premier, de sorte qu'il possède des nombres algébriques conjugués distincts de lui-même.

L'ensemble des nombres algébriques est un sous-champ du champ des nombres complexes. Autrement dit, la somme, la différence, le produit et le quotient de deux nombres algébriques sont des nombres algébriques.

En effet, soient deux nombres algébriques α et β. Désignons par $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ et par $\beta_1 = \beta, \beta_2, \ldots, \beta_s$, respectivement, les nombres conjugués de α et de β; soient $f(x)$ et $g(x)$ les polynômes irréductibles à coefficients rationnels ayant pour zéros respectivement α et β. Formons un polynôme ayant pour zéros les sommes $\alpha_i + \beta_j$; c'est le polynôme

$$\varphi(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} [x - (\alpha_i + \beta_j)].$$

Ses coefficients sont invariants par rapport aux permutations des zéros α_i et des zéros β_j. Par conséquent, les coefficients de ce polynôme sont, en vertu du théorème sur les polynômes symétriques par rapport à deux groupes d'indéterminées (cf. fin du § 53), des polynômes des coefficients de $f(x)$ et de $g(x)$. Autrement dit, les coeffi-

[1] Il ne faut pas confondre cette notion avec celle des nombres conjugués omplexes.

cients de $\varphi(x)$ sont rationnels, de sorte que le nombre $\alpha + \beta = \alpha_1 + \beta_1$, zéro de $\varphi(x)$, est algébrique.

De la même manière, utilisant les polynômes

$$\psi(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} [x - (\alpha_i - \beta_j)]$$

et

$$\chi(x) = \prod_{i=1}^{n} \prod_{j=1}^{s} (x - \alpha_i \beta_j)$$

on démontre que $\alpha - \beta$ et $\alpha\beta$ sont algébriques.

Pour démontrer que le quotient est aussi algébrique il suffit de montrer que, α étant algébrique et non nul, il en est de même pour α^{-1}. Soit α zéro du polynôme à coefficients rationnels

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n.$$

Alors, il est clair que le polynôme

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

qui est aussi à coefficients rationnels, a pour zéro le nombre α^{-1}, ce qu'il fallait démontrer.

Du théorème démontré il résulte que la somme d'un nombre rationnel et d'un radical, par exemple $1 + \sqrt[3]{2}$, ainsi que la somme de deux radicaux, par exemple $\sqrt{3} + \sqrt[7]{5}$, sont des nombres algébriques. Toutefois, nous ne pouvons pas pour le moment affirmer que les nombres qui s'écrivent sous forme de radicaux superposés d'un nombre algébrique, par exemple $\sqrt{1 + \sqrt{2}}$, sont algébriques. Cela découlera du *théorème* suivant:

Supposons que ω soit un zéro d'un polynôme dont les coefficients sont des nombres algébriques

$$\varphi(x) = x^n + \alpha x^{n-1} + \beta x^{n-2} + \ldots + \lambda x + \mu,$$

alors ω est aussi un nombre algébrique.

Soient $\alpha_i, \beta_j, \ldots, \lambda_s, \mu_t$ les nombres conjugués respectivement de $\alpha, \beta, \ldots, \lambda, \mu$; en outre $\alpha_1 = \alpha$, $\beta_1 = \beta, \ldots, \lambda_1 = \lambda$, $\mu_1 = \mu$. Considérons les polynômes de la forme

$$\varphi_{i, j, \ldots, s, t}(x) = x^n + \alpha_i x^{n-1} + \beta_j x^{n-2} + \ldots + \lambda_s x + \mu_t,$$

en particulier, $\varphi_{1, 1, \ldots, 1, 1}(x) = \varphi(x)$; formons le produit de ces polynômes

$$F(x) = \prod_{i, j, \ldots, s, t} \varphi_{i, j, \ldots, s, t}(x).$$

Il est clair que les coefficients du polynôme $F(x)$ sont symétriques par rapport à chaque groupe d'indéterminées $\alpha_i, \beta_j, \ldots, \lambda_s, \mu_t$,

de sorte que (de nouveau, en vertu du théorème correspondant du § 53) ces coefficients sont des polynômes des coefficients des polynômes irréductibles (à coefficients rationnels) ayant pour zéros respectivement α, β, . . ., λ, μ, c'est-à-dire les coefficients de $F(x)$ sont aussi rationnels. Le nombre ω étant un zéro de $\varphi(x)$, il est, par conséquent, un zéro du polynôme $F(x)$ à coefficients rationnels, c'est-à-dire ω est un nombre algébrique.

Appliquons ce théorème au nombre $\omega = \sqrt{1+\sqrt{2}}$. Le nombre $\alpha = 1 + \sqrt{2}$ étant, d'après le théorème précédent, algébrique, le nombre ω est un zéro du polynôme $x^2 - \alpha$ à coefficients algébriques, c'est-à-dire ce nombre est algébrique. De façon générale, appliquant à plusieurs reprises les deux théorèmes que nous venons de démontrer, le lecteur sera facilement conduit au résultat:

Tout nombre qui s'exprime par des radicaux sur le champ des nombres rationnels (c'est-à-dire qui s'exprime au moyen d'un nombre fini de radicaux superposés de manière quelconque) est un nombre algébrique.

Il est clair que les nombres algébriques s'exprimant par des radicaux forment un champ. Néanmoins, il faut garder présent à l'esprit que, en vertu de la remarque faite à la fin du § 38 (non démontrée), ce champ n'est qu'un sous-champ du champ des nombres algébriques.

On a déjà signalé ci-dessus que les nombres e et π sont transcendants. Il s'avère qu'il y a une infinité de nombres transcendants. De plus, utilisant les notions et méthodes de la théorie des ensembles, nous montrerons qu'il existe, dans un certain sens, plus de nombres transcendants que de nombres algébriques; par la suite le sens exact de cette affirmation sera clair.

Un ensemble infini M est dit *dénombrable* s'il existe une application bijective entre les éléments de M et les nombres naturels, c'est-à-dire si les éléments de M peuvent être numérotés au moyen des nombres entiers positifs; dans le cas contraire, l'ensemble M est dit *non dénombrable.*

Lemme 1. *Tout ensemble infini M contient un sous-ensemble dénombrable.*

En effet, soit a_1 un élément de M. Choisissons dans M un élément a_2 ne coïncidant pas avec a_1. De façon générale, soient $a_1, a_2, \ldots, a_n$ des éléments distincts de M. L'ensemble M étant infini, il ne peut pas être épuisé par les éléments choisis, de sorte que l'on peut indiquer dans M un élément a_{n+1} ne coïncidant pas avec $a_1, a_2, \ldots, a_n$. Continuant ce processus, nous trouverons dans M un sous-ensemble infini composé d'éléments

$$a_1, a_2, \ldots, a_n, \ldots$$

ce sous-ensemble est manifestement dénombrable.

Lemme 2. *Tout sous-ensemble infini B d'un ensemble dénombrable A est dénombrable.*

L'ensemble A étant dénombrable, on peut l'écrire sous la forme d'une suite

$$a_1, a_2, \ldots, a_n, \ldots \tag{1}$$

Soient a_{k_1} le premier élément de la suite (1) appartenant à l'ensemble B, a_{k_2}, le second élément ayant cette propriété, etc. Posant $a_{k_n} = b_n$, $n = 1, 2, \ldots$,

nous pouvons écrire le sous-ensemble B sous la forme de la suite

$$b_1, b_2, \ldots, b_n, \ldots,$$

ce qui démontre que B est dénombrable.

Lemme 3. *La réunion dénombrable d'ensembles finis disjoints deux à deux est dénombrable.*

En effet, soient les ensembles finis

$$A_1, A_2, \ldots, A_n, \ldots$$

et soit B leur réunion. Il est clair qu'on arrive à numéroter les éléments de l'ensemble B en procédant de la manière suivante : on numérote de manière quelconque les éléments de A_1 et l'on continue à numéroter les éléments de B en passant aux éléments de A_2, etc.

Lemme 4. *La réunion de deux ensembles dénombrables disjoints est dénombrable.*

Soient deux ensembles dénombrables A d'éléments

$$a_1, a_2, \ldots, a_n, \ldots$$

et B d'éléments

$$b_1, b_2, \ldots, b_n, \ldots$$

et soit C leur réunion. Posant

$$a_n = c_{2n-1}, \ b_n = c_{2n}, \qquad n = 1, 2 \ldots,$$

les éléments de l'ensemble C se trouvent mis sous la forme d'une suite

$$c_1, c_2, \ldots, c_{2n-1}, c_{2n}, \ldots,$$

ce qui démontre que C est dénombrable.

Démontrons maintenant le *théorème* :

L'ensemble des nombres algébriques est dénombrable.

Démontrons d'abord que *l'ensemble des polynômes à coefficients entiers dépendant d'une indéterminée est dénombrable.* Soit

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

un tel polynôme non nul ; appelons *hauteur* de ce polynôme le nombre naturel

$$h_f = n + |a_0| + |a_1| + \ldots + |a_{n-1}| + |a_n|.$$

Il est clair que le nombre de polynômes à coefficients entiers ayant la même hauteur h est fini ; désignons cet ensemble par M_h. En outre, désignons par M_0 l'ensemble composé de l'unique polynôme nul. L'ensemble des polynômes à coefficients entiers est la réunion dénombrable des ensembles finis M_0, M_1, M_2, . . ., M_h, . . . ; d'après le lemme 3, l'ensemble des polynômes à coefficients entiers est dénombrable.

Il en résulte, vu le lemme 2, que *l'ensemble des polynômes irréductibles primitifs est aussi dénombrable.* Or, on sait que tout nombre algébrique est zéro d'un et seulement d'un polynôme irréductible primitif. Donc, réunissant les zéros de tous ces polynômes, c'est-à-dire formant une réunion dénombrable d'ensembles finis, nous obtenons l'ensemble des nombres algébriques ; vu le lemme 3, cet ensemble est dénombrable.

Enfin, démontrons le *théorème* :

L'ensemble des nombres transcendants est non dénombrable.

Considérons d'abord l'ensemble F de nombres réels x, compris entre zéro et l'unité, $0 < x < 1$, et montrons que *cet ensemble est non dénombrable*. Il est connu que tout x, compris entre 0 et 1, peut être mis sous la forme d'une fraction décimale infinie

$$x = 0,\ \alpha_1\alpha_2 \ldots \alpha_n \ldots ;$$

de plus, cette écriture est bien définie si l'on convient d'éliminer les écritures telles que $\alpha_n = 9$ pour tout n à partir d'une certaine valeur $n = N$; inversement, toute fraction du type indiqué coïncide avec un certain nombre x appartenant à l'ensemble F. Supposons maintenant que F soit dénombrable, c'est-à-dire que les nombres x puissent être mis sous la forme d'une suite

$$x_1,\ x_2,\ \ldots,\ x_k,\ \ldots \tag{2}$$

Soit

$$x_k = 0,\ \alpha_{k_1},\ \alpha_{k_2} \ldots \alpha_{k_n} \ldots$$

l'écriture du nombre x_k sous la forme d'une fraction décimale infinie correspondante. Ecrivons la fraction décimale infinie

$$0,\ \beta_1\beta_2 \ldots \beta_n \ldots, \tag{3}$$

prenant β_1 différente de la première décimale de la fraction x_1, soit $\beta_1 \neq \alpha_{11}$, puis, prenant β_2 différente de la seconde décimale du nombre x_2, soit $\beta_2 \neq \alpha_{22}$, et, plus généralement, soit $\beta_n \neq \alpha_{nn}$. En outre, choisissons les β_n de manière qu'il y ait une infinité de décimales β_n différentes de 9. Il est clair qu'il existe une fraction (3) satisfaisant à toutes ces conditions. Par conséquent, la fraction (3) est un nombre de l'ensemble F ; or, en vertu de son choix, la fraction (3) est différente de tous les nombres de la suite (2). Cette contradiction démontre que l'ensemble F est non dénombrable.

Il en résulte que *l'ensemble des nombres complexes est non dénombrable* ; en effet, supposant le contraire, l'ensemble des nombres complexes, vu le lemme 2, ne pourrait pas contenir le sous-ensemble non dénombrable F. Maintenant, vu le lemme 4, il est clair que l'ensemble des nombres transcendants est non dénombrable, car la réunion de cet ensemble et de l'ensemble dénombrable des nombres algébriques donne l'ensemble des nombres complexes, qui est non dénombrable.

Les deux théorèmes que nous avons démontrés montrent, vu le lemme 1, que l'ensemble des nombres transcendants est, en réalité, beaucoup plus riche en éléments, c'est-à-dire il est de « puissance » beaucoup plus grande que l'ensemble des nombres algébriques.

Chapitre XIII — FORME NORMALE DES MATRICES

§ 59. Equivalence des λ-matrices

Nous revenons, une fois de plus, aux problèmes se rapportant à l'algèbre linéaire. Etudiant le chapitre VII, le lecteur a déjà eu l'occasion de constater le rôle important tenu par la notion de matrices semblables. Notamment, deux matrices carrées d'ordre n sont semblables si et seulement si elles donnent une même application linéaire (rapportée à deux bases différentes) dans un espace vectoriel à n dimensions. Mais jusqu'ici nous ne savons pas encore dire si deux matrices données sont semblables ou non. D'autre part, nous ne savons pas non plus indiquer, parmi les matrices semblables à une matrice donnée A, celle qui a, dans un certain sens, la forme la plus simple; de plus, même le problème d'équivalence d'une matrice à une matrice diagonale n'a été étudié au § 33 que dans un cas particulier. C'est justement ces problèmes que nous considérerons dans ce chapitre; en outre, le champ de base P sera supposé quelconque.

Occupons-nous d'abord des matrices carrées d'ordre n dont les éléments sont des polynômes d'une indéterminée λ de degré quelconque à coefficients dans un champ P. Ces matrices sont dites *polynomiales* ou encore *λ-matrices*. La matrice caractéristique $A - \lambda E$ d'une matrice carrée A à éléments dans un champ P fournit un exemple de λ-matrices; les éléments de la diagonale principale de $A - \lambda E$ sont des polynômes du premier degré et les autres éléments des polynômes de degré nul ou des zéros. Toute matrice à éléments dans un champ P (pour abréger nous l'appelons *numérique*) est un cas particulier de λ-matrice, car ses éléments sont des polynômes de degré nul ou des zéros.

Soit une λ-matrice

$$A(\lambda) = \begin{pmatrix} a_{11}(\lambda) & \dots & a_{1n}(\lambda) \\ \cdot & \cdot\cdot\cdot\cdot\cdot & \cdot \\ a_{n1}(\lambda) & \dots & a_{nn}(\lambda) \end{pmatrix}.$$

Les *transformations* suivantes de cette matrice sont dites *élémentaires*:

1) multiplication d'une ligne de la matrice $A(\lambda)$ par un élément α non nul d'un champ P;

2) multiplication d'une colonne de la matrice $A(\lambda)$ par un élément α non nul d'un champ P;

3) addition de la $j^{\text{ème}}$ ligne, multipliée par un polynôme $\varphi(\lambda)$ de l'anneau $P[\lambda]$, à la $i^{\text{ème}}$ ligne de la matrice $A(\lambda)$, i et j étant quelconques, $i \neq j$;

4) addition de la $j^{\text{ème}}$ colonne, multipliée par un polynôme $\varphi(\lambda)$ de l'anneau $P[\lambda]$, à la $i^{\text{ème}}$ colonne de la matrice $A(\lambda)$, i et j étant quelconques, $i \neq j$.

Il est facile de voir que *toute transformation élémentaire d'une λ-matrice est inversible et a pour inverse une transformation élémentaire.* Ainsi, la transformation 1) a pour inverse la multiplication de la même ligne par α^{-1}, qui existe et est une transformation élémentaire car $\alpha \neq 0$. La transformation inverse de 3) consiste à additionner la $j^{\text{ème}}$ ligne, multipliée par $-\varphi(\lambda)$, à la $i^{\text{ème}}$ ligne de $A(\lambda)$.

On peut, au moyen des transformations élémentaires, échanger tout couple de lignes ou de colonnes d'une matrice $A(\lambda)$.

Supposons, par exemple, que l'on doive échanger la $i^{\text{ème}}$ et la $j^{\text{ème}}$ ligne de la matrice $A(\lambda)$. On peut le faire au moyen de quatre transformations élémentaires, comme le montre le schéma:

$$\begin{pmatrix} i \\ j \end{pmatrix} \to \begin{pmatrix} i+j \\ j \end{pmatrix} \to \begin{pmatrix} i+j \\ -i \end{pmatrix} \to \begin{pmatrix} j \\ -i \end{pmatrix} \to \begin{pmatrix} j \\ i \end{pmatrix}.$$

Ici on effectue successivement les transformations: a) on ajoute la $j^{\text{ème}}$ ligne à la $i^{\text{ème}}$ ligne; b) puis on retranche la $i^{\text{ème}}$ ligne ainsi obtenue de la $j^{\text{ème}}$ ligne; c) on ajoute après cela la $i^{\text{ème}}$ ligne à la $j^{\text{ème}}$ ligne; d) ensuite, on multiplie la $j^{\text{ème}}$ ligne par -1.

Nous dirons que deux λ-matrices $A(\lambda)$ et $B(\lambda)$ sont *équivalentes* et écrirons $A(\lambda) \sim B(\lambda)$ si l'on peut obtenir la matrice $B(\lambda)$ en appliquant à $A(\lambda)$ un nombre fini de transformations élémentaires. La relation d'équivalence ainsi définie est manifestement réflexive et transitive; en outre, elle est symétrique car toute transformation élémentaire est inversible. Autrement dit, *l'ensemble des λ-matrices carrées d'ordre n sur un champ P est la réunion des classes disjointes de matrices équivalentes.*

Notre but immédiat est de trouver, parmi les λ-matrices équivalentes à une matrice $A(\lambda)$, celle qui a la forme la plus simple. Introduisons pour cela la notion suivante. Une *λ-matrice* est dite *canonique* si elle jouit des trois propriétés suivantes:

a) cette matrice est diagonale, c'est-à-dire elle est de la forme

$$\begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}; \qquad (1)$$

b) tout polynôme $e_i(\lambda)$ est divisible par $e_{i-1}(\lambda)$, et cela pour tout i, $i = 2, 3, \ldots, n$;

c) le coefficient du terme principal de tout polynôme $e_i(\lambda)$ non nul, $i = 1, 2, \ldots, n$, est égal à l'unité.

Supposons que parmi les polynômes $e_i(\lambda)$ de la diagonale principale d'une λ-matrice canonique (1) il y ait des polynômes identiquement nuls; alors, d'après la propriété b), ces polynômes nuls se trouvent en bas de la diagonale principale. D'autre part, s'il y a des polynômes de degré nul parmi les polynômes $e_i(\lambda)$, d'après la propriété c), tous ces polynômes de degré nul coïncident avec l'unité et, d'après la propriété b), ils se trouvent en haut de la diagonale principale.

En particulier, il y a des λ-matrices numériques, y compris la matrice nulle et la matrice unité, qui sont canoniques.

Toute λ-matrice est équivalente à une λ-matrice canonique, c'est-à-dire toute λ-matrice peut être réduite par des transformations élémentaires à une forme canonique.

Démontrons ce théorème par récurrence sur l'ordre n des λ-matrices considérées. En effet, pour $n = 1$, on a

$$A(\lambda) = (a(\lambda)).$$

Si $a(\lambda) = 0$, alors la matrice $A(\lambda)$ est déjà canonique. Si, par contre, $a(\lambda) \neq 0$, il suffit alors de diviser le polynôme $a(\lambda)$ par le coefficient de son terme principal — ce qui est une transformation élémentaire — pour obtenir une matrice canonique.

Supposons que le théorème soit vrai pour les λ-matrices d'ordre $n - 1$. Considérons une λ-matrice $A(\lambda)$ d'ordre n. Si elle est nulle, c'est qu'elle est déjà canonique et il n'y a rien à démontrer. Par conséquent, supposons que parmi les éléments de la matrice $A(\lambda)$ il y a des polynômes non nuls.

Permutant, s'il est nécessaire, des lignes et des colonnes de la matrice $A(\lambda)$, on peut faire passer l'un de ses éléments non nuls dans l'angle gauche supérieur. Aussi, parmi les λ-matrices équivalentes à la matrice $A(\lambda)$ il y a celles qui ont un polynôme non nul situé à l'intersection de la première ligne et de la première colonne. Considérons toutes ces matrices. Les polynômes se trouvant dans l'angle gauche supérieur de ces matrices sont de degrés différents. Or, le degré d'un polynôme est un nombre entier non négatif et tout ensemble non vide de nombres entiers non négatifs possède un nombre entier minimal. Par conséquent, on peut trouver, parmi les λ-matrices équivalentes à la matrice $A(\lambda)$, une λ-matrice telle que le polynôme situé dans l'angle gauche supérieur soit non nul et de degré minimal. Divisant la première ligne de la matrice indiquée par le coefficient du terme principal de ce polynôme, nous

obtenons une λ-matrice équivalente à la matrice $A(\lambda)$, soit

$$A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & b_{12}(\lambda) & \dots & b_{1n}(\lambda) \\ b_{21}(\lambda) & b_{22}(\lambda) & \dots & b_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ b_{n1}(\lambda) & b_{n2}(\lambda) & \dots & b_{nn}(\lambda) \end{pmatrix},$$

et telle que $e_1(\lambda) \neq 0$, le coefficient du terme principal de $e_1(\lambda)$ étant l'unité; en outre, *aucune superposition de transformations élémentaires de la matrice trouvée ne peut donner une matrice dont l'élément de l'angle gauche supérieur soit un polynôme non nul de degré inférieur à celui de* $e_1(\lambda)$.

Montrons que *tous les éléments de la première ligne et de la première colonne de la matrice ci-dessus sont divisibles par* $e_1(\lambda)$. Par exemple, soit

$$b_{1j}(\lambda) = e_1(\lambda)\, q(\lambda) + r(\lambda),$$

avec $2 \leqslant j \leqslant n$, où le degré de $r(\lambda)$ (si $r(\lambda)$ n'est pas nul) est inférieur à celui de $e_1(\lambda)$. Retranchant de la $j^{\text{ème}}$ colonne de la matrice sa première colonne multipliée par $q(\lambda)$ et échangeant ensuite la première et la $j^{\text{ème}}$ colonne, nous sommes conduits à une matrice équivalente à la matrice $A(\lambda)$ et telle que son élément de l'angle gauche supérieur soit le polynôme $r(\lambda)$, c'est-à-dire le polynôme de degré inférieur à celui de $e_1(\lambda)$, ce qui est en contradiction avec le choix de ce polynôme. Il en résulte que $r(\lambda) = 0$, ce qu'il fallait démontrer.

Retranchant maintenant de la $j^{\text{ème}}$ colonne de la matrice sa première colonne multipliée par $q(\lambda)$, nous annulons l'élément $b_{1j}(\lambda)$. Effectuant ces transformations élémentaires pour $j = 2, 3, \dots, n$, nous annulons tous les éléments $b_{1j}(\lambda)$. De la même manière on peut annuler tous les éléments $b_{i1}(\lambda)$ avec $i = 2, 3, \dots$ $\dots, n$. *Finalement, nous sommes conduits à une matrice équivalente à la matrice* $A(\lambda)$ *et telle que son élément de l'angle gauche supérieur soit* $e_1(\lambda)$ *et tous les autres éléments de la première ligne et de la première colonne soient nuls*,

$$A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & 0 & \dots & 0 \\ 0 & c_{22}(\lambda) & \dots & c_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ 0 & c_{n2}(\lambda) & \dots & c_{nn}(\lambda) \end{pmatrix}. \qquad (2)$$

En vertu de l'hypothèse de récurrence, la matrice d'ordre $(n - 1)$ située dans l'angle droit inférieur de la matrice (2) peut être réduite

par des transformations élémentaires à la forme canonique:

$$\begin{pmatrix} c_{22}(\lambda) & \dots & c_{2n}(\lambda) \\ \dots & \dots & \dots \\ c_{n2}(\lambda) & \dots & c_{nn}(\lambda) \end{pmatrix} \sim \begin{pmatrix} e_2(\lambda) & & 0 \\ & \ddots & \\ 0 & & e_n(\lambda) \end{pmatrix}.$$

Appliquant ces transformations aux lignes et colonnes correspondantes de la matrice (2) (la première ligne et la première colonne sont conservées par les transformations en question), nous obtenons

$$A(\lambda) \sim \begin{pmatrix} e_1(\lambda) & & & 0 \\ & e_2(\lambda) & & \\ & & \ddots & \\ 0 & & & e_n(\lambda) \end{pmatrix}. \tag{3}$$

Pour démontrer que la matrice (3) est canonique il reste à montrer que $e_2(\lambda)$ est divisible par $e_1(\lambda)$. Supposons que

$$e_2(\lambda) = e_1(\lambda)\, q(\lambda) + r(\lambda),$$

avec $r(\lambda) \neq 0$, le degré de $r(\lambda)$ étant inférieur à celui de $e_1(\lambda)$. Or, ajoutant à la seconde colonne de la matrice (3) sa première colonne multipliée par $q(\lambda)$ et retranchant ensuite la première ligne de la seconde, nous remplaçons l'élément $e_2(\lambda)$ par l'élément $r(\lambda)$. Echangeant ensuite les deux premières lignes et les deux premières colonnes, nous faisons passer l'élément $r(\lambda)$ dans l'angle gauche supérieur, ce qui contredit, toutefois, le choix du polynôme $e_1(\lambda)$.

Le théorème sur la réduction d'une λ-matrice à la forme canonique est démontré. Ce théorème doit être complété par le *théorème d'unicité*:

Toute λ-matrice est équivalente à une matrice canonique définie de façon unique.

En effet, soit une λ-matrice $A(\lambda)$ d'ordre n. Fixons un nombre entier k, $1 \leqslant k \leqslant n$, et considérons les mineurs d'ordre k de la matrice $A(\lambda)$. Calculant ces mineurs, nous obtenons une famille finie de polynômes de λ; désignons par $d_k(\lambda)$ le plus grand commun diviseur de cette famille, le coefficient du terme principal de $d_k(\lambda)$ étant l'unité.

Donc, nous avons les polynômes

$$d_1(\lambda),\ d_2(\lambda),\ \dots,\ d_n(\lambda), \tag{4}$$

bien définis par la matrice $A(\lambda)$. Ici $d_1(\lambda)$ est le plus grand commun diviseur des éléments de la matrice $A(\lambda)$, le coefficient du terme principal de $d_1(\lambda)$ étant l'unité, et $d_n(\lambda)$ est le déterminant de la matrice $A(\lambda)$ divisé par le coefficient de son terme principal. Remar-

quons encore que si la matrice $A(\lambda)$ est de rang r, alors

$$d_{r+1}(\lambda) = \ldots = d_n(\lambda) = 0,$$

tandis que tous les autres polynômes de la famille (4) sont non nuls.

Le plus grand commun diviseur $d_k(\lambda)$ de tous les mineurs d'ordre k d'une λ-matrice $A(\lambda)$, $k = 1, 2, \ldots, n$, est conservé par les transformations élémentaires.

Cette proposition est presque évidente lorsqu'il s'agit des transformations élémentaires 1) et 2). Aussi, multipliant, par exemple, la $i^{\text{ème}}$ ligne de la matrice $A(\lambda)$ par un nombre α du champ P, $\alpha \neq 0$, les mineurs d'ordre k contenant des éléments de la $i^{\text{ème}}$ ligne se trouvent multipliés par α, et tous les autres mineurs d'ordre k sont conservés. Or, lorsqu'on calcule le plus grand commun diviseur d'une famille de polynômes, on peut les multiplier par les éléments non nuls du champ P.

Passons maintenant aux transformations élémentaires 3) et 4). Supposons, par exemple, qu'on ajoute à la $i^{\text{ème}}$ ligne de la matrice $A(\lambda)$ sa $j^{\text{ème}}$ ligne multipliée par un polynôme $\varphi(\lambda)$, $i \neq j$. Désignons par $\overline{A}(\lambda)$ la matrice obtenue par cette transformation et notons par $\overline{d}_k(\lambda)$ le plus grand commun diviseur (à coefficient l'unité pour le terme principal) des mineurs d'ordre k de la matrice $\overline{A}(\lambda)$. Voyons ce que deviennent les mineurs d'ordre k de la matrice $A(\lambda)$ après cette transformation.

Il est clair que les mineurs ne contenant pas les éléments de la $i^{\text{ème}}$ ligne ne changent pas. Les mineurs contenant simultanément des éléments de la $i^{\text{ème}}$ et de la $j^{\text{ème}}$ ligne ne changent pas non plus, car le déterminant ne varie pas lorsqu'on ajoute à l'une de ses lignes une autre ligne multipliée par un nombre. Enfin, considérons un mineur d'ordre k qui contient des éléments de la $i^{\text{ème}}$ ligne, mais ne contient pas ceux de la $j^{\text{ème}}$ ligne; notons-le par M. Il est clair que le mineur correspondant de la matrice $\overline{A}(\lambda)$ peut être représenté comme la somme du mineur M et du produit de $\varphi(\lambda)$ par le mineur M' de la matrice $A(\lambda)$, qui s'obtient du mineur M en remplaçant les éléments de la $i^{\text{ème}}$ ligne par les éléments correspondants de la $j^{\text{ème}}$ ligne de $A(\lambda)$. M et M' étant divisibles par $d_k(\lambda)$, il en est de même pour $M + \varphi(\lambda) M'$.

Il en résulte que tout mineur d'ordre k de la matrice $\overline{A}(\lambda)$ est divisible par $d_k(\lambda)$, de sorte que $\overline{d}_k(\lambda)$ est également divisible par $d_k(\lambda)$. La transformation élémentaire ci-dessus étant inversible et ayant pour inverse une transformation du même type, $d_k(\lambda)$ est divisible par $\overline{d}_k(\lambda)$. Vu que les coefficients des termes principaux des polynômes $\overline{d}_k(\lambda)$ et $d_k(\lambda)$ sont l'unité, on a $\overline{d}_k(\lambda) = d_k(\lambda)$, ce qu'il fallait démontrer.

Ainsi, *à toute λ-matrice équivalente à une matrice $A(\lambda)$ correspond une même famille de polynômes* (4). En particulier, ceci est vrai pour toute matrice canonique équivalente à $A(\lambda)$. Soit (3) une telle matrice.

Calculons les polynômes $d_k(\lambda)$, $k = 1, 2, \ldots, n$, en partant de la matrice (3). Il est clair que le mineur d'ordre k situé dans l'angle gauche supérieur de cette matrice est égal au produit

$$e_1(\lambda)\, e_2(\lambda) \ldots e_k(\lambda). \tag{5}$$

Ensuite, un mineur d'ordre k de la matrice (3) se trouvant à l'intersection des lignes et des colonnes d'indices $i_1, i_2, \ldots, i_k$, avec $i_1 < i_2 < \ldots < i_k$, est égal au produit $e_{i_1}(\lambda)\, e_{i_2}(\lambda) \ldots e_{i_k}(\lambda)$ qui est divisible par le produit (5). En effet, vu que $1 \leqslant i_1$, $e_{i_1}(\lambda)$ est divisible par $e_1(\lambda)$, puis, vu que $2 \leqslant i_2$, $e_{i_2}(\lambda)$ est divisible par $e_2(\lambda)$, etc. Enfin, tout mineur d'ordre k de la matrice (3) tel qu'au moins pour un indice i il contienne des éléments de la $i^{\text{ème}}$ ligne mais ne contienne pas ceux de la $i^{\text{ème}}$ colonne est nul car il possède une ligne nulle.

Il en résulte que le produit (5) est le plus grand commun diviseur des mineurs d'ordre k de la matrice (3) et, par conséquent, de la matrice initiale $A(\lambda)$,

$$d_k(\lambda) = e_1(\lambda)\, e_2(\lambda) \ldots e_k(\lambda), \qquad k = 1, 2, \ldots, n. \tag{6}$$

A présent, il est facile de montrer que les *polynômes $e_k(\lambda)$, $k = 1, 2, \ldots, n$, sont bien définis par la matrice $A(\lambda)$. Soit r le rang de cette matrice.* On sait que dans ce cas $d_r(\lambda) \neq 0$, tandis que $d_{r+1}(\lambda) = 0$, de sorte que, vu (6), $e_{r+1}(\lambda) = 0$. Il en résulte, d'après les propriétés d'une matrice canonique, que pour une *matrice $A(\lambda)$ de rang r inférieur à n* les égalités suivantes ont toujours lieu:

$$e_{r+1}(\lambda) = e_{r+2}(\lambda) = \ldots = e_n(\lambda) = 0. \tag{7}$$

D'autre part, pour $k \leqslant r$ on déduit de (6), vu que $d_{k-1}(\lambda) \neq 0$, la formule

$$e_k(\lambda) = \frac{d_k(\lambda)}{d_{k-1}(\lambda)}. \tag{8}$$

Ceci achève la démonstration de l'unicité de la matrice canonique équivalente à une λ-matrice donnée. En même temps nous avons donné un procédé permettant de calculer les polynômes $e_k(\lambda)$, dits *facteurs invariants* de la matrice $A(\lambda)$.

Exemple. Réduire à la forme canonique la λ-matrice

$$A(\lambda) = \begin{pmatrix} \lambda^3 - \lambda & 2\lambda^2 \\ \lambda^2 + 5\lambda & 3\lambda \end{pmatrix}.$$

Réalisant les transformations élémentaires, on obtient successivement :

$$A(\lambda) \sim \begin{pmatrix} \lambda^3 - \lambda & \frac{2}{3}\lambda^2 \\ \lambda^2 + 5\lambda & \lambda \end{pmatrix} \sim \begin{pmatrix} \frac{1}{3}\lambda^3 - \frac{10}{3}\lambda^2 - \lambda & 0 \\ \lambda^2 + 5\lambda & \lambda \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \frac{1}{3}\lambda^3 - \frac{10}{3}\lambda_2 - \lambda & 0 \\ 0 & \lambda \end{pmatrix} \sim \begin{pmatrix} \lambda^3 - 10\lambda^2 - 3\lambda & 0 \\ 0 & \lambda \end{pmatrix} \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^3 - 10\lambda^2 - 3\lambda \end{pmatrix}.$$

D'autre part, on pourrait calculer directement les facteurs invariants de la matrice $A(\lambda)$. Notamment, en calculant le plus grand commun diviseur des éléments de cette matrice, on trouve :

$$d_1(\lambda) = e_1(\lambda) = \lambda.$$

Calculant le déterminant de la matrice $A(\lambda)$ et remarquant que le coefficient de son terme principal est l'unité, nous obtenons :

$$d_2(\lambda) = \lambda^4 - 10\lambda^3 - 3\lambda^2,$$

de sorte que

$$e_2(\lambda) = \frac{d_2(\lambda)}{d_1(\lambda)} = \lambda^3 - 10\lambda^2 - 3\lambda.$$

§ 60. λ-matrices unimodulaires. Matrices numériques semblables et équivalence de leurs matrices caractéristiques

Des résultats du paragraphe précédent découle un critère d'équivalence des λ-matrices qui peut être énoncé des deux manières presque identiques :

Deux λ-matrices sont équivalentes si et seulement si elles sont réductibles à une même forme canonique.

Deux λ-matrices sont équivalentes si et seulement si elles possèdent les mêmes facteurs invariants.

Etablissons encore un critère de tout autre nature.

On sait que la matrice unité E appartient à la classe des λ-matrices canoniques. Une λ-matrice $U(\lambda)$ est appelée *unimodulaire* si elle a E pour matrice canonique ou encore si tous ses facteurs invariants coïncident avec l'unité.

Une λ-matrice $U(\lambda)$ est unimodulaire si et seulement si son déterminant est non nul et ne dépend pas de λ, c'est-à-dire si son déterminant est un élément non nul du champ de base P.

En effet, si $U(\lambda) \sim E$, alors à ces deux matrices correspond un même polynôme $d_n(\lambda)$. Or, pour la matrice unité on a : $d_n(\lambda) = 1$. Il en découle que le déterminant de la matrice $U(\lambda)$, coïncidant avec $d_n(\lambda)$ à un facteur numérique près, est un élément non nul du champ P. Inversement, si le déterminant d'une matrice $U(\lambda)$ est non nul et ne dépend pas de λ, alors le polynôme $d_n(\lambda)$ correspondant à cette matrice est l'unité, donc, vu (6) du paragraphe précé

dent, les facteurs invariants $e_i(\lambda)$ de la matrice $U(\lambda)$ coïncident avec l'unité pour $i = 1, 2, \ldots, n$.

Il s'ensuit que *toute matrice numérique non dégénérée est une λ-matrice unimodulaire.* Toutefois les λ-matrices unimodulaires peuvent avoir une structure très compliquée. Aussi, la λ-matrice

$$\begin{pmatrix} \lambda & \lambda^3+5 \\ \lambda^2-\lambda-4 & \lambda^4-\lambda^3-4\lambda^2+5\lambda-5 \end{pmatrix}$$

est unimodulaire, son déterminant étant égal à 20, c'est-à-dire étant non nul et ne dépendant pas de λ.

Du théorème démontré ci-dessus résulte que *le produit de deux λ-matrices unimodulaires est une λ-matrice unimodulaire*; en effet, il suffit de rappeler que le déterminant du produit de deux matrices est le produit de leurs déterminants.

Une λ-matrice $U(\lambda)$ est unimodulaire si et seulement si elle est inversible et a pour inverse une λ-matrice.

En effet, soit une λ-matrice non dégénérée; calculant son inverse par la méthode ordinaire, nous devons diviser les cofacteurs des éléments de cette matrice par son déterminant, c'est-à-dire par un polynôme de λ. Pour cette raison, les éléments de la matrice inverse sont, généralement, des fractions rationnelles et non des polynômes de λ, c'est-à-dire, dans ce cas, *la matrice inverse n'est plus une λ-matrice.* Une λ-matrice étant unimodulaire, il faut, pour calculer la matrice inverse, diviser les cofacteurs de ses éléments par un nombre non nul du champ P; par conséquent, les éléments de la matrice inverse sont des polynômes de λ, de sorte qu'elle est une λ-matrice. Réciproquement, supposons qu'une λ-matrice $U(\lambda)$ a pour inverse la λ-matrice $U^{-1}(\lambda)$; les déterminants de ces matrices étant des polynômes par rapport à λ et leur produit étant l'unité, il en résulte que chaque déterminant est un polynôme de degré nul.

De la dernière remarque découle un complément au théorème que nous venons de démontrer:

Une λ-matrice inverse d'une λ-matrice unimodulaire est unimodulaire.

La notion de matrice unimodulaire est utilisée pour formuler le *critère suivant d'équivalence des λ-matrices*:

Deux λ-matrices $A(\lambda)$ et $B(\lambda)$ d'ordre n sont équivalentes si et seulement si il existe deux λ-matrices unimodulaires $U(\lambda)$ et $V(\lambda)$ *d'ordre n telles que l'on ait*

$$B(\lambda) = U(\lambda)\, A(\lambda)\, V(\lambda). \qquad (1)$$

Introduisons d'abord une notion qui sera utilisée au cours de la démonstration de ce critère. Appelons *matrice élémentaire* une matri-

ce numérique (et, par conséquent, une λ-matrice) qui est de la forme

$$\begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ \cdots & \cdots & \alpha & \cdots & \cdots \\ & & & 1 & \\ & & & & \ddots \\ 0 & & & & 1 \end{pmatrix} (i); \qquad (2)$$

une matrice élémentaire (2) a la même structure que la matrice unité à cette différence près que le $i^{\text{ème}}$ élément de la diagonale principale, $1 \leqslant i \leqslant n$, n'est plus l'unité, mais un nombre *non nul* α du champ P. D'autre part, appelons également *matrice élémentaire* une λ-matrice ayant la même forme que la matrice unité à cette différence près qu'à l'intersection de sa $i^{\text{ème}}$ ligne et de sa $j^{\text{ème}}$ colonne se trouve un polynôme $\varphi(\lambda)$ de l'anneau $P[\lambda]$:

$$\begin{pmatrix} 1 & & \vdots & & \\ & \ddots & \vdots & & \\ \cdots & 1 & \cdots \varphi(\lambda) & \cdots & \\ & & \vdots & & \\ & & 1 & & \\ & & \vdots & \ddots & \\ & & \vdots & & 1 \end{pmatrix} (i), \qquad (3)$$
$$(j)$$

ici $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, $i \neq j$.

Toute matrice élémentaire est unimodulaire. En effet, le déterminant de la matrice (2) est α, et $\alpha \neq 0$, d'après notre hypothèse; le déterminant de la matrice (3) est l'unité.

L'application d'une transformation élémentaire à une λ-matrice $A(\lambda)$ est équivalente à la multiplication, soit à gauche, soit à droite, de la matrice $A(\lambda)$ par une matrice élémentaire.

En effet, le lecteur peut vérifier facilement que les quatre propositions suivantes sont vraies: 1) la multiplication à gauche de la matrice $A(\lambda)$ par une matrice (2) est équivalente à la multiplication de la $i^{\text{ème}}$ ligne de $A(\lambda)$ par le nombre α; 2) la multiplication à droite de la matrice $A(\lambda)$ par une matrice (2) est équivalente à la multiplication de la $i^{\text{ème}}$ colonne de $A(\lambda)$ par le nombre α; 3) la multiplication à gauche de la matrice $A(\lambda)$ par une matrice (3) est équivalente à ce qu'on ajoute à la $i^{\text{ème}}$ ligne de $A(\lambda)$ sa $j^{\text{ème}}$ ligne multipliée par $\varphi(\lambda)$; 4) la multiplication à droite de la matrice $A(\lambda)$

par une matrice (3) est équivalente à ce qu'on ajoute à la $j^{\text{ème}}$ colonne de $A(\lambda)$ sa $i^{\text{ème}}$ colonne multipliée par $\varphi(\lambda)$.

Passons maintenant à la *démonstration du critère d'équivalence des λ-matrices*. Soit $A(\lambda) \sim B(\lambda)$; alors, on peut passer de $A(\lambda)$ à $B(\lambda)$ appliquant à $A(\lambda)$ un nombre fini de transformations élémentaires. Remplaçant chacune de ces transformations par la multiplication à gauche ou à droite par une matrice élémentaire, nous sommes conduits à l'égalité

$$B(\lambda) = U_1(\lambda) \ldots U_k(\lambda) A(\lambda) V_1(\lambda) \ldots V_l(\lambda), \tag{4}$$

où les matrices $U_1(\lambda), \ldots, U_k(\lambda), V_1(\lambda), \ldots, V_l(\lambda)$ sont élémentaires et, par conséquent, unimodulaires. Ainsi, les matrices

$$U(\lambda) = U_1(\lambda) \ldots U_k(\lambda), \quad V(\lambda) = V_1(\lambda) \ldots V_l(\lambda), \tag{5}$$

produits des matrices unimodulaires, sont encore unimodulaires, de sorte que l'égalité (4) peut être récrite sous la forme (1). Notons que si, par exemple, $k = 0$, c'est-à-dire si les transformations élémentaires étaient appliquées aux colonnes, alors on pose $U(\lambda) = E$.

La partie démontrée du critère permet d'énoncer le résultat suivant:

Une λ-matrice est unimodulaire si et seulement si elle est le produit d'un nombre fini de matrices élémentaires.

En effet, nous avons déjà exploité le fait que le produit de matrices élémentaires est une matrice unimodulaire. Inversement, soit une matrice unimodulaire $W(\lambda)$; alors $W(\lambda)$ est équivalente à la matrice unité E. Répétant la démonstration donnée ci-dessus avec les matrices E et $W(\lambda)$ au lieu des matrices $A(\lambda)$ et $B(\lambda)$, la formule (4) donne

$$W(\lambda) = U_1(\lambda) \ldots U_k(\lambda) V_1(\lambda) \ldots V_l(\lambda),$$

c'est-à-dire la matrice $W(\lambda)$ est représentée sous la forme d'un produit de matrices élémentaires.

Il est facile maintenant de *démontrer la réciproque de notre critère*. Soient deux matrices $A(\lambda)$ et $B(\lambda)$ et supposons qu'il existe deux matrices unimodulaires $U(\lambda)$ et $V(\lambda)$ telles que l'on ait (1). On a déjà démontré que les matrices $U(\lambda)$ et $V(\lambda)$ peuvent être représentées sous la forme d'un produit de matrices élémentaires; supposons que ce soient les représentations (5). L'égalité (1) prend alors la forme (4) et, remplaçant dans (4) toute matrice élémentaire par la transformation élémentaire correspondante, nous obtenons finalement que $A(\lambda) \sim B(\lambda)$.

Polynômes matriciels. On peut considérer la notion de λ-matrice d'un autre point de vue. Appelons *λ-polynôme matriciel d'ordre n sur un champ P* un polynôme par rapport à λ dont les coefficients sont des matrices carrées d'un même ordre n à éléments dans le champ P;

voici sa forme générale:

$$A_0\lambda^k + A_1\lambda^{k-1} + \ldots + A_{k-1}\lambda + A_k. \qquad (6)$$

Interprétant le produit de la matrice A_i par λ^{k-i}, conformément au § 15, comme le produit de chaque élément de A_i par λ^{k-i} et additionnant les matrices dans (6) d'après ce même § 15, nous constatons que *tout λ-polynôme matriciel d'ordre n peut être mis sous la forme d'une λ-matrice d'ordre n*. Ainsi,

$$\begin{pmatrix} 4 & 0 \\ -1 & 1 \end{pmatrix}\lambda^3 + \begin{pmatrix} 0 & -3 \\ 0 & 1 \end{pmatrix}\lambda^2 + \begin{pmatrix} 1 & 2 \\ 0 & -2 \end{pmatrix}\lambda + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 4\lambda^3+\lambda & -3\lambda^2+2\lambda+1 \\ -\lambda^3 & \lambda^3+\lambda^2-2\lambda \end{pmatrix}.$$

Inversement, *toute λ-matrice d'ordre n peut être représentée sous la forme d'un λ-polynôme matriciel d'ordre n*. Ainsi,

$$\begin{pmatrix} 3\lambda^2-5 & \lambda+1 \\ \lambda^4+2\lambda & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\lambda^4 + \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}\lambda^2 + \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\lambda + \begin{pmatrix} -5 & 1 \\ 0 & -3 \end{pmatrix}.$$

La correspondance entre les λ-matrices et les λ-polynômes matriciels est bijective et même isomorphe au sens du § 46. En effet, l'égalité des λ-polynômes de la forme (6) est équivalente à l'égalité des coefficients matriciels des mêmes puissances de λ, et la multiplication d'une matrice par λ est équivalente à la multiplication de cette matrice par la matrice scalaire ayant λ pour éléments de la diagonale principale.

Soit une λ-matrice $A(\lambda)$,

$$A(\lambda) = A_0\lambda^k + A_1\lambda^{k-1} + \ldots + A_{k-1}\lambda + A_k,$$

où la matrice A_0 est non nulle. L'entier k est appelé *degré* de la λ-matrice $A(\lambda)$; il est clair que k est le plus haut degré en λ des éléments de $A(\lambda)$.

L'interprétation des λ-matrices comme des polynômes matriciels permet de développer la théorie de la divisibilité des λ-matrices analogue à celle des polynômes numériques; bien entendu, la noncommutativité de la multiplication des matrices et l'existence de diviseurs de zéro compliquent cette théorie. Nous nous bornerons à la considération de l'*algorithme de division avec reste*.

Soient deux λ-matrices d'ordre n sur un champ P

$$A(\lambda) = A_0\lambda^k + A_1\lambda^{k-1} + \ldots + A_{k-1}\lambda + A_k,$$
$$B(\lambda) = B_0\lambda^l + B_1\lambda^{l-1} + \ldots + B_{l-1}\lambda + B_l;$$

en outre, supposons que la matrice B_0 soit non dégénérée, c'est-à-dire que la matrice B_0^{-1} existe. Alors on peut indiquer deux λ-matrices $Q_1(\lambda)$

et $R_1(\lambda)$ d'ordre n sur le champ P telles que l'on ait

$$A(\lambda) = B(\lambda) Q_1(\lambda) + R_1(\lambda), \tag{7}$$

avec degré de $R_1(\lambda)$ inférieur à celui de $B(\lambda)$ ou bien avec $R_1(\lambda) = 0$. D'autre part, on peut trouver deux λ-matrices d'ordre n sur le champ P telles que

$$A(\lambda) = Q_2(\lambda) B(\lambda) + R_2(\lambda), \tag{8}$$

le degré de $R_2(\lambda)$ étant inférieur à celui de $B(\lambda)$ ou bien $R_2(\lambda)$ étant la matrice nulle. Les matrices $Q_1(\lambda)$, $R_1(\lambda)$ et $Q_2(\lambda)$, $R_2(\lambda)$ vérifiant respectivement les égalités (7) *et* (8) *sont bien définies.*

La démonstration de ce théorème est en tous points semblable à celle du théorème analogue sur les polynômes numériques (cf. § 20). Supposons, par exemple, que la condition (7) soit satisfaite encore par un couple de matrices $\overline{Q}_1(\lambda)$ et $\overline{R}_1(\lambda)$, le degré de $\overline{R}_1(\lambda)$ étant inférieur à celui de $B(\lambda)$. Alors on a

$$B(\lambda)[Q_1(\lambda) - \overline{Q}_1(\lambda)] = \overline{R}_1(\lambda) - R_1(\lambda).$$

Le degré du second membre est inférieur à l, tandis que le degré du premier membre, sous l'hypothèse que la matrice entre crochets soit non nulle, est, vu que la matrice B_0 est non dégénérée, supérieur ou égal à l. Il en résulte l'unicité des matrices $Q_1(\lambda)$ et $R_1(\lambda)$.

Notons, pour démontrer l'existence de ces matrices, que le degré de la différence

$$A(\lambda) - B(\lambda) \cdot B_0^{-1} A_0 \lambda^{k-l}$$

est, pour $k \geqslant l$, strictement inférieur à k; par conséquent, $B_0^{-1} A_0 \lambda^{k-l}$ est le terme principal du λ-polynôme matriciel $Q_1(\lambda)$. On continue la démonstration comme au § 20. D'autre part, le degré de la différence

$$A(\lambda) - A_0 B_0^{-1} \lambda^{k-l} \cdot B(\lambda)$$

est aussi strictement inférieur à k, c'est-à-dire que $A_0 B_0^{-1} \lambda^{k-l}$ est le terme principal du λ-polynôme matriciel $Q_2(\lambda)$. Nous constatons que, effectivement, les λ-matrices $Q_1(\lambda)$ et $Q_2(\lambda)$ (ainsi que $R_1(\lambda)$ et $R_2(\lambda)$) sont, dans le cas général, différentes.

Théorème fondamental des matrices semblables. Nous avons déjà signalé ci-dessus que nous n'avions pas de moyen efficace pour dire si deux matrices numériques (c'est-à-dire à éléments dans un champ de base P) A et B sont semblables ou non. D'autre part, leurs matrices caractéristiques $A - \lambda E$ et $B - \lambda E$ étant des λ-matrices, le problème d'équivalence de ces matrices peut être résolu de façon efficace. Aussi est-il facile de comprendre l'importance du théorème suivant.

Deux matrices A et B à éléments dans un champ P sont semblables si et seulement si leurs matrices caractéristiques $A - \lambda E$ et *$B - \lambda E$ sont équivalentes.*

En effet, soient deux matrices semblables A et B; autrement dit, il existe une matrice C non dégénérée sur le champ P telle que

$$B = C^{-1}AC.$$

Alors

$$C^{-1}(A - \lambda E)\,C = C^{-1}AC - \lambda\,(C^{-1}EC) = B - \lambda E.$$

Or, les matrices numériques non dégénérées C^{-1} et C sont des λ-matrices unimodulaires. Nous voyons que la matrice $B - \lambda E$ est égale à la matrice $A - \lambda E$ multipliée respectivement à gauche et à droite par deux matrices unimodulaires, c'est-à-dire $A - \lambda E \sim \sim B - \lambda E$.

La démonstration de la réciproque est plus compliquée. Soit

$$A - \lambda E \sim B - \lambda E.$$

Alors, il existe des matrices unimodulaires $U(\lambda)$ et $V(\lambda)$ telles que l'on ait

$$U(\lambda)(A - \lambda E)\,V(\lambda) = B - \lambda E. \tag{9}$$

Vu que les matrices unimodulaires sont inversibles et ont pour inverses des λ-matrices, déduisons de (9) les égalités suivantes qui seront utilisées plus tard:

$$\left.\begin{aligned} U(\lambda)(A - \lambda E) &= (B - \lambda E)\,V^{-1}(\lambda),\\ (A - \lambda E)\,V(\lambda) &= U^{-1}(\lambda)(B - \lambda E). \end{aligned}\right\} \tag{10}$$

La λ-matrice $B - \lambda E$ étant du premier degré en λ et le coefficient du terme principal du polynôme matriciel correspondant étant la matrice non dégénérée $-E$, l'algorithme de division avec reste est applicable aux matrices $U(\lambda)$ et $B - \lambda E$: il existe, donc, deux matrices $Q_1(\lambda)$ et R_1 (la matrice R_1 est de degré nul en λ si elle n'est pas nulle, c'est-à-dire R_1 ne dépend pas de λ) telles que

$$U(\lambda) = (B - \lambda E)\,Q_1(\lambda) + R_1. \tag{11}$$

De même, on a

$$V(\lambda) = Q_2(\lambda)(B - \lambda E) + R_2. \tag{12}$$

On déduit de (9), utilisant (11) et (12), l'égalité

$$\begin{aligned} R_1(A - \lambda E)\,R_2 = (B - \lambda E) - U(\lambda)(A - \lambda E)\,Q_2(\lambda)(B - \lambda E) -\\ -(B - \lambda E)\,Q_1(\lambda)(A - \lambda E)\,V(\lambda) +\\ +(B - \lambda E)\,Q_1(\lambda)(A - \lambda E)\,Q_2(\lambda)(B - \lambda E) \end{aligned}$$

ou, d'après (10), l'égalité

$$R_1(A-\lambda E)R_2=(B-\lambda E)-(B-\lambda E)V^{-1}(\lambda)Q_2(\lambda)(B-\lambda E)-$$
$$-(B-\lambda E)Q_1(\lambda)U^{-1}(\lambda)(B-\lambda E)+$$
$$+(B-\lambda E)Q_1(\lambda)(A-\lambda E)Q_2(\lambda)(B-\lambda E)=$$
$$=(B-\lambda E)\{E-[V^{-1}(\lambda)Q_2(\lambda)+$$
$$+Q_1(\lambda)U^{-1}(\lambda)-Q_1(\lambda)(A-\lambda E)Q_2(\lambda)](B-\lambda E)\}.$$

La matrice entre crochets dans le second membre est, en réalité, nulle; en effet, supposant le contraire, cette matrice serait une λ-matrice, puisque $V^{-1}(\lambda)$ et $U^{-1}(\lambda)$ sont des λ-matrices, et, par conséquent, elle serait de degré au moins nul, et le degré de la matrice entre accolades serait au moins 1, de sorte que le degré du second membre serait au moins 2. Or, cela est impossible, vu que le premier membre est une λ-matrice de degré 1.

Ainsi,

$$R_1(A-\lambda E)R_2=B-\lambda E,$$

d'où, identifiant les coefficients matriciels des mêmes puissances de λ, il vient:

$$R_1AR_2=B, \tag{13}$$

$$R_1R_2=E. \tag{14}$$

L'égalité (14) montre non seulement que la matrice R_2 est non nulle, mais aussi qu'elle est non dégénérée; en outre,

$$R_2^{-1}=R_1,$$

alors l'égalité (13) prend la forme

$$R_2^{-1}AR_2=B,$$

ce qui démontre que les matrices A et B sont semblables.

En même temps, nous *avons trouvé le moyen de calculer la matrice non dégénérée R_2, transmuant la matrice A en la matrice B*. Notamment, les matrices $A-\lambda E$ et $B-\lambda E$ étant équivalentes, la première se réduit à la seconde par un nombre fini de transformations élémentaires. Choisissons parmi ces transformations celles qui sont appliquées aux colonnes et notons par $V(\lambda)$ le produit des matrices élémentaires correspondantes, l'ordre des facteurs devant être conservé. Ensuite, divisons $V(\lambda)$ par $B-\lambda E$ de manière que le quotient précède le diviseur (cf. (8)). Le reste de la division est la matrice R_2.

En réalité, on peut éviter cette division si l'on utilise le lemme suivant, qui trouvera aussi d'autres applications dans le § 62:

Lemme. *Soit*

$$V(\lambda)=V_0\lambda^s+V_1\lambda^{s-1}+\ldots+V_{s-1}\lambda+V_s,\quad V_0\neq 0. \tag{15}$$

Si

$$\begin{aligned} V(\lambda)&=(\lambda E-B)\,Q_1(\lambda)+R_1,\\ V(\lambda)&=Q_2(\lambda)\,(\lambda E-B)+R_2,\end{aligned} \tag{16}$$

alors

$$\begin{aligned} R_1&=B^sV_0+B^{s-1}V_1+\ldots+BV_{s-1}+V_s,\\ R_2&=V_0B^s+V_1B^{s-1}+\ldots+V_{s-1}B+V_s.\end{aligned} \tag{17}$$

Il suffit de démontrer au moins la première partie du lemme, car la seconde se démontre de facon tout à fait analogue. La démonstration se ramène à la vérification directe de l'égalité (16), en remplaçant le polynôme $V(\lambda)$ par son expression (15), R_1 par la formule (17) et prenant pour $Q_1(\lambda)$ le polynôme

$$Q_1(\lambda)=V_0\lambda^{s-1}+(BV_0+V_1)\,\lambda^{s-2}+(B^2V_0+BV_1+V_2)\,\lambda^{s-3}+\ldots$$
$$\ldots+(B^{s-1}V_0+B^{s-2}V_1+\ldots+V_{s-1}).$$

On laisse au lecteur le soin de le vérifier.

Exemple. Soient deux matrices

$$A=\begin{pmatrix}-2 & 1\\ 0 & 3\end{pmatrix},\qquad B=\begin{pmatrix}-10 & -4\\ 26 & 11\end{pmatrix}$$

Leurs matrices caractéristiques sont équivalentes, car elles se réduisent à la même forme canonique

$$\begin{pmatrix}1 & 0\\ 0 & \lambda^2-\lambda-6\end{pmatrix},$$

par conséquent, les matrices A et B sont semblables.

Pour calculer la matrice R_2 transmuant A en B, trouvons une famille de transformations élémentaires réduisant $A-\lambda E$ à $B-\lambda E$. Ainsi,

$$A-\lambda E\begin{pmatrix}-2-\lambda & 1\\ 0 & 3-\lambda\end{pmatrix}\sim\begin{pmatrix}-2-\lambda & 1\\ -16-8\lambda & 11-\lambda\end{pmatrix}\sim$$
$$\sim\begin{pmatrix}8+4\lambda & -4\\ -16-8\lambda & 11-\lambda\end{pmatrix}\sim\begin{pmatrix}40+4\lambda & -4\\ -104 & 11-\lambda\end{pmatrix}\sim\begin{pmatrix}-10-\lambda & -4\\ 26 & 11-\lambda\end{pmatrix}=B-\lambda E.$$

Il n'y a que les deux dernières transformations qui sont appliquées aux colonnes: on ajoute à la première colonne la seconde multipliée par -8, puis on multiplie la première colonne par $-\frac{1}{4}$. Le produit des matrices élémentaires cor-

respondantes est

$$V(\lambda)=\begin{pmatrix}1 & 0\\ -8 & 1\end{pmatrix}\begin{pmatrix}-\frac{1}{4} & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-\frac{1}{4} & 0\\ 2 & 1\end{pmatrix}.$$

Cette matrice ne dépendant pas de λ, elle est la matrice R_2 cherchée.

Evidemment, la matrice transmuant A en B n'est pas unique. Par exemple, la matrice

$$\begin{pmatrix}3 & 1\\ 2 & 1\end{pmatrix}$$

transmue également A en B.

§ 61. Forme normale de Jordan

Nous allons considérer l'ensemble des matrices carrées d'ordre n à éléments dans un champ P. Définissant dans cet ensemble un type spécial de matrices, appelées matrices *de Jordan*, nous montrerons qu'une classe assez large de matrices carrées a pour formes normales des matrices de Jordan. Notamment, *pour qu'une matrice carrée soit semblable à une matrice de Jordan ou, comme on dit, soit réductible à la forme normale de Jordan, il faut et il suffit que les racines caractéristiques de cette matrice appartiennent au champ de base P.* Choisissant pour P le champ des nombres complexes, il en résultera que *toute matrice à éléments nombres complexes est réductible sur le champ des nombres complexes à la forme normale de Jordan.*

Introduisons les définitions nécessaires. On appelle *cellule de Jordan* d'ordre k associée à un nombre λ_0 une matrice d'ordre k $1 \leqslant k \leqslant n$, qui est de la forme

$$\begin{pmatrix}\lambda_0 & 1 & & & 0\\ & \lambda_0 & 1 & & \\ & & \cdot & \cdot & \\ & & & \cdot & 1\\ 0 & & & & \lambda_0\end{pmatrix}; \qquad (1)$$

autrement dit, la diagonale principale de cette matrice a pour éléments le nombre λ_0 répété k fois ; la ligne parallèle, la plus proche de la diagonale principale, située au-dessus de cette dernière, a pour éléments l'unité répétée $k - 1$ fois ; tous les autres éléments de la

matrice (1) sont des zéros. Ainsi, les matrices

$$(\lambda_0), \quad \begin{pmatrix} \lambda_0 & 1 \\ 0 & \lambda_0 \end{pmatrix}, \quad \begin{pmatrix} \lambda_0 & 1 & 0 \\ 0 & \lambda_0 & 1 \\ 0 & 0 & \lambda_0 \end{pmatrix}$$

sont des cellules de Jordan, respectivement, du premier, du deuxième et du troisième ordre.

On appelle *matrice de Jordan* d'ordre n une matrice de la forme

$$J = \begin{pmatrix} \boxed{J_1} & & & 0 \\ & \boxed{J_2} & & \\ & & \ddots & \\ 0 & & & \boxed{J_s} \end{pmatrix}; \tag{2}$$

ici les sous-matrices $J_1, J_2, \ldots, J_s$ situées le long de la diagonale principale sont les cellules de Jordan associées à des nombres du champ P (qui ne sont pas forcément tous distincts), les ordres des cellules n'étant pas nécessairement tous différents. Les éléments de la matrice (2) n'appartenant pas aux cellules J_k sont tous nuls. En outre, $s \geqslant 1$, c'est-à-dire une cellule de Jordan d'ordre n est une matrice de Jordan du même ordre, et il est clair que $s \leqslant n$.

Bien que cela ne sera pas utilisé par la suite, notons quand même que la structure d'une matrice de Jordan peut être décrite sans recourir à la notion de cellule de Jordan. Notamment, il est clair qu'une matrice J est une matrice de Jordan si et seulement si elle est de la forme

$$\begin{pmatrix} \lambda_1 & \varepsilon_1 & & & 0 \\ & \lambda_2 & \varepsilon_2 & & \\ & & \ddots & \ddots & \\ & & & \ddots & \varepsilon_{n-1} \\ 0 & & & & \lambda_n \end{pmatrix},$$

avec λ_i, $i = 1, 2, \ldots, n$, éléments du champ P, et ε_j, $j = 1, 2, \ldots, n-1$, zéro ou unité; en outre, si $\varepsilon_j = 1$, alors $\lambda_j = \lambda_{j+1}$.

Les matrices diagonales sont un cas particulier des matrices de Jordan; ce sont, effectivement, les matrices de Jordan dont toutes les cellules de Jordan sont d'ordre 1.

Notre but immédiat est de *calculer la forme canonique de la matrice caractéristique $J - \lambda E$ d'une matrice de Jordan J d'ordre n*. Trouvons d'abord la forme canonique de la matrice caractéristique d'une cellule de Jordan (1) d'ordre k:

$$\begin{pmatrix} \lambda_0-\lambda & 1 & & & 0 \\ & \lambda_0-\lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ 0 & & & & \lambda_0-\lambda \end{pmatrix} \qquad (3)$$

Calculant le déterminant de cette matrice et se rappelant que le coefficient du terme principal du polynôme $d_k(\lambda)$ doit être l'unité, nous trouvons

$$d_k(\lambda) = (\lambda - \lambda_0)^k.$$

D'autre part, parmi les mineurs d'ordre $k - 1$ de la matrice (3) il y en a un égal à l'unité, à savoir le mineur qui s'obtient en éliminant la première colonne et la dernière ligne de la matrice (3). Ainsi,

$$d_{k-1}(\lambda) = 1.$$

Il en résulte que *la forme canonique de la matrice* (3) *est la λ-matrice d'ordre k*:

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & (\lambda-\lambda_0)^k \end{pmatrix} \qquad (4)$$

Démontrons maintenant le *lemme*.

Si les polynômes $\varphi_1(\lambda)$, $\varphi_2(\lambda)$, ..., $\varphi_t(\lambda)$ de l'anneau $P[\lambda]$ sont deux à deux premiers entre eux, alors on a l'équivalence:

$$\begin{pmatrix} \varphi_1(\lambda) & & & 0 \\ & \varphi_2(\lambda) & & \\ & & \ddots & \\ 0 & & & \varphi_t(\lambda) \end{pmatrix} \sim \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \prod_{i=1}^{t} \varphi_i(\lambda) \end{pmatrix}.$$

Il suffit, évidemment, de considérer le cas de $t=2$. Les polynômes $\varphi_1(\lambda)$ et $\varphi_2(\lambda)$ étant premiers entre eux, il existe dans l'anneau $P[\lambda]$ des polynômes $u_1(\lambda)$ et $u_2(\lambda)$ tels que

$$\varphi_1(\lambda)\,u_1(\lambda)+\varphi_2(\lambda)\,u_2(\lambda)=1.$$

Par conséquent, on a

$$\begin{pmatrix} \varphi_1(\lambda) & 0 \\ 0 & \varphi_2(\lambda) \end{pmatrix} \sim \begin{pmatrix} \varphi_1(\lambda) & \varphi_1(\lambda)\,u_1(\lambda) \\ 0 & \varphi_2(\lambda) \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} \varphi_1(\lambda) & \varphi_1(\lambda)\,u_1(\lambda)+\varphi_2(\lambda)\,u_2(\lambda) \\ 0 & \varphi_2(\lambda) \end{pmatrix} = \begin{pmatrix} \varphi_1(\lambda) & 1 \\ 0 & \varphi_2(\lambda) \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & \varphi_1(\lambda) \\ \varphi_2(\lambda) & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & \varphi_1(\lambda) \\ 0 & -\varphi_1(\lambda)\,\varphi_2(\lambda) \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 \\ 0 & -\varphi_1(\lambda)\,\varphi_2(\lambda) \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & \varphi_1(\lambda)\,\varphi_2(\lambda) \end{pmatrix},$$

ce qu'il fallait démontrer.

Passons maintenant à la considération de la matrice caractéristique d'une matrice de Jordan J de la forme (2):

$$J-\lambda E=\begin{pmatrix} \boxed{J_1-\lambda E_1} & & & 0 \\ & \boxed{J_2-\lambda E_2} & & \\ & & \ddots & \\ 0 & & & \boxed{J_s-\lambda E_s} \end{pmatrix}; \qquad (5)$$

ici E_i est une matrice unité du même ordre que J_i, $i = 1, 2, \ldots, s$. Soient $\lambda_1, \lambda_2, \ldots, \lambda_t$, $t \leqslant s$, des nombres *distincts* auxquels sont associées les cellules de Jordan de la matrice J. Supposons, ensuite, que le nombre de cellules de Jordan associées au nombre λ_i soit q_i, $q_i \geqslant 1$, et que les ordres des cellules, disposés suivant leur ordre de décroissance, soient

$$k_{i1} \geqslant k_{i2} \geqslant \ldots \geqslant k_{iq_i}; \tag{6}$$

ici $i = 1, 2, \ldots, t$. Notons que

$$\sum_{i=1}^{t} q_i = s,$$

$$\sum_{i=1}^{t} \sum_{j=1}^{q_i} k_{ij} = n$$

bien que l'on n'utilisera pas ces égalités.

Appliquant les transformations élémentaires aux lignes et colonnes de la matrice (5) qui engendrent la cellule $J_i - \lambda E_i$, nous ne touchons manifestement pas aux autres cellules diagonales. Il en résulte que la matrice (5) peut être réduite au moyen de transformations élémentaires à la forme où toute cellule $J_i - \lambda E_i$, $i = 1, 2, \ldots, s$, est remplacée par une cellule de la forme (4). Autrement dit, *la matrice $J - \lambda E$ est équivalente à une matrice diagonale dont les éléments diagonaux sont, à part un certain nombre d'unités, les polynômes suivants qui correspondent à toutes les cellules de Jordan de la matrice J:*

$$\left.\begin{array}{l} (\lambda-\lambda_1)^{k_{11}},\ (\lambda-\lambda_1)^{k_{12}},\ \ldots,\ (\lambda-\lambda_1)^{k_{1q_1}}, \\ (\lambda-\lambda_2)^{k_{21}},\ (\lambda-\lambda_2)^{k_{22}},\ \ldots,\ (\lambda-\lambda_2)^{k_{2q_2}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (\lambda-\lambda_t)^{k_{t1}},\ (\lambda-\lambda_t)^{k_{t2}},\ \ldots,\ (\lambda-\lambda_t)^{k_{tq_t}}. \end{array}\right\} \tag{7}$$

Nous n'indiquons pas ici les places occupées par les polynômes (7) dans la diagonale principale, car les éléments diagonaux de toute λ-matrice diagonale peuvent être déplacés en échangeant des lignes et des colonnes de même indice. Cette remarque doit être prise en considération dans ce qui suit.

Soit q le maximum des nombres q_i, $i = 1, 2, \ldots, t$. Désignons par $e_{n-j+1}(\lambda)$ le produit des polynômes qui composent la $j^{\text{ème}}$ colonne du tableau (7), $j = 1, 2, \ldots, q$, c'est-à-dire

$$e_{n-j+1}(\lambda) = \prod_{i=1}^{t} (\lambda-\lambda_i)^{k_{ij}}, \tag{8}$$

en outre, si certains éléments de la $j^{\text{ème}}$ colonne dans (7) sont absents (cela peut se produire lorsque $q_i < j$ pour certain indice i), alors

les facteurs correspondants dans le produit (8) doivent être l'unité. Les nombres $\lambda_1, \lambda_2, \ldots, \lambda_t$ étant, d'après notre hypothèse, distincts. les puissances des binômes linéaires, éléments de la $j^{\text{ème}}$ colonne du tableau (7), sont deux à deux premières entre elles. Par conséquent, vu le lemme démontré ci-dessus, ces puissances peuvent être remplacées, au moyen de transformations élémentaires de la matrice, par leur produit $e_{n-j+1}(\lambda)$ et par un certain nombre d'éléments unité.

Réalisant ceci pour $j = 1, 2, \ldots, q$, nous obtenons

$$J - \lambda E \sim \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & e_{n-q+1}(\lambda) & & & \\ & & & & \ddots & & \\ & & & & & e_{n-1}(\lambda) & \\ 0 & & & & & & e_n(\lambda) \end{pmatrix}. \qquad (9)$$

C'est là la forme canonique cherchée d'une matrice $J - \lambda E$. En effet, les coefficients des termes principaux des polynômes, éléments diagonaux de la matrice (9), sont tous l'unité et chacun de ces polynômes, vu la condition (6), est divisible par le polynôme qui le précède.

Exemple. Soit

$$J = \begin{pmatrix} \boxed{\begin{matrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{matrix}} & & & & 0 \\ & \boxed{2} & & & \\ & & \boxed{\begin{matrix} 5 & 1 \\ 0 & 5 \end{matrix}} & & \\ & & & \boxed{\begin{matrix} 5 & 1 \\ 0 & 5 \end{matrix}} & \\ 0 & & & & \boxed{2} \end{pmatrix}.$$

Le tableau des polynômes (7), correspondant à cette matrice de Jordan d'ordre 9, est de la forme

$$(\lambda-2)^3, \quad \lambda-2, \quad \lambda-2,$$
$$(\lambda-5)^2, \quad (\lambda-5)^2.$$

Par conséquent, les facteurs invariants de la matrice J sont les polynômes

$$e_9(\lambda) = (\lambda-2)^3(\lambda-5)^2,$$
$$e_8(\lambda) = (\lambda-2)(\lambda-5)^2,$$
$$e_7(\lambda) = \lambda-2,$$

tandis que $e_6(\lambda) = \ldots = e_1(\lambda) = 1$.

A présent que nous avons appris à reconstituer, à partir d'une matrice de Jordan J, la forme canonique de sa matrice caractéristique, nous pouvons démontrer le théorème suivant:

Deux matrices de Jordan sont semblables si et seulement si elles sont formées par les mêmes cellules de Jordan, c'est-à-dire si, les cellules de Jordan étant les mêmes, seule leur disposition le long de la diagonale principale des deux matrices peut être différente.

En effet, le tableau des polynômes (7) est bien défini par les cellules de Jordan d'une matrice de Jordan J; en outre, le tableau (7) ne dépend pas de la disposition des cellules le long de la diagonale principale de cette matrice, de sorte que deux matrices de Jordan J et J' ayant les mêmes cellules de Jordan possèdent le même tableau des polynômes (7) correspondant et, par conséquent, les mêmes polynômes (8). Ainsi, les matrices caractéristiques $J - \lambda E$ et $J' - \lambda E$ ont les mêmes facteurs invariants, c'est-à-dire qu'elles sont équivalentes; donc, les matrices J et J' sont semblables.

Inversement, deux matrices de Jordan J et J' étant semblables, leurs matrices caractéristiques possèdent les facteurs invariants identiques. Soient les polynômes (8), $j = 1, 2, \ldots, q$, ceux des facteurs invariants qui sont différents de l'unité. Or, les polynômes (8) permettent de reconstituer le tableau des polynômes (7). Notamment, les polynômes (8) se décomposent en un produit des puissances des facteurs linéaires, vu que, comme on l'a déjà démontré, les facteurs invariants de la matrice caractéristique d'une matrice de Jordan possèdent cette propriété. Le tableau (7) est juste composé des puissances maximales des facteurs linéaires qui font partie de la décomposition des polynômes (8). Enfin, à partir du tableau (7) on peut reconstituer les cellules de Jordan des matrices de Jordan initialement données; en effet, à tout polynôme $(\lambda - \lambda_i)^{k_{ij}}$ du tableau (7) correspond une cellule de Jordan d'ordre k_{ij} associée au nombre λ_i. Ceci démontre que les matrices J et J' sont composées des mêmes cellules de Jordan dont la disposition peut être différente dans J et J'.

En particulier, il résulte de ce théorème que *toute matrice de Jordan semblable à une matrice diagonale est elle-même diagonale et que deux matrices diagonales sont semblables si et seulement si l'une d'elles s'obtient de l'autre en échangeant des éléments de la diagonale principale.*

Réduction des matrices à la forme normale de Jordan. Soit une matrice A à éléments dans un champ P, *réductible à la forme normale de Jordan*, c'est-à-dire A est semblable à une matrice de Jordan; alors il résulte du théorème démontré ci-dessus qu'*une forme normale de Jordan de A est bien définie à une disposition des cellules de Jordan le long de la diagonale principale près*. La condition pour qu'une matrice A admette une telle réduction est donnée dans le théorème qui suit; de plus, la démonstration de ce théorème donne un moyen pratique de trouver la matrice de Jordan semblable à la matrice A, à condition, toutefois, qu'une telle matrice de Jordan existe. Notons en outre que la *réductibilité de A sur un champ P* signifie que les éléments de la matrice transmuant A en la forme de Jordan appartiennent à P.

Une matrice A à éléments dans un champ P est réductible sur le champ P à la forme normale de Jordan si et seulement si toutes ses racines caractéristiques appartiennent au champ de base P.

En effet, si une matrice A est semblable à une matrice de Jordan, alors ces deux matrices possèdent les mêmes racines caractéristiques. Or, il n'y a pas de difficulté à calculer les racines caractéristiques de la matrice J: le déterminant de la matrice $J - \lambda E$ étant le produit des éléments de la diagonale principale, le polynôme $|J - \lambda E|$ se décompose sur le champ P en un produit de facteurs linéaires et ses zéros coïncident avec les nombres, éléments diagonaux de la matrice J.

Réciproquement, supposons que les racines caractéristiques de la matrice A soient des éléments du champ de base P. Soient

$$e_{n-q+1}(\lambda), \ \ldots, \ e_{n-1}(\lambda), \ e_n(\lambda) \tag{10}$$

les facteurs invariants de la matrice $A-\lambda E$ différents de l'unité; alors

$$|A-\lambda E| = (-1)^n e_{n-q+1}(\lambda) \ \ldots \ e_{n-1}(\lambda) e_n(\lambda).$$

En effet, le déterminant de la matrice $A - \lambda E$ et celui de la matrice canonique de $A - \lambda E$ doivent coïncider à un facteur numérique près qui est, en réalité, $(-1)^n$, car tel est le coefficient du terme principal du polynôme caractéristique $|A - \lambda E|$. Ainsi, parmi les polynômes (10) il n'y a pas de polynômes nuls, la somme des degrés de ces polynômes est n et ils se décomposent tous, sur le champ P, en un produit de facteurs linéaires (la dernière propriété résulte de la supposition que le polynôme $|A - \lambda E|$ possède une telle décomposition).

Soient (8) les décompositions des polynômes (10) en un produit des puissances des facteurs linéaires. Appelons *diviseurs élémentaires du polynôme e_{n-j+1}* les puissances des binômes linéaires distincts intervenant dans la décomposition (8) de e_{n-j+1}, $j = 1, 2, \ldots, q$

(on ne considère que les puissances différentes de l'unité), c'est-à-dire les diviseurs élémentaires sont les polynômes

$$(\lambda - \lambda_1)^{k_{1j}}, \ (\lambda - \lambda_2)^{k_{2j}}, \ \ldots, \ (\lambda - \lambda_t)^{k_{tj}}.$$

Les diviseurs élémentaires de tous les polynômes (10) sont dits *diviseurs élémentaires de la matrice* A ; écrivons-les sous la forme d'un tableau (7).

Prenons maintenant une matrice de Jordan d'ordre n composée des cellules de Jordan définies de la manière suivante : *à tout diviseur élémentaire* $(\lambda - \lambda_i)^{k_{ij}}$ *de la matrice* A *nous faisons correspondre une cellule de Jordan d'ordre* k_{ij} *associée au nombre* λ_i. Il est clair que les facteurs invariants, différents de l'unité, de la matrice $J - \lambda E$ sont les polynômes (10) et seulement ces polynômes. Ainsi, les matrices $A - \lambda E$ et $J - \lambda E$ sont équivalentes et, par conséquent, les matrices A et J sont semblables.

Exemple. Soit une matrice

$$A = \begin{pmatrix} -16 & -17 & 87 & -108 \\ 8 & 9 & -42 & 54 \\ -3 & -3 & 16 & -18 \\ -1 & -1 & 6 & -8 \end{pmatrix}$$

Réduisant de la manière ordinaire la matrice $A - \lambda E$ à la forme canonique, nous trouvons que les facteurs invariants (différents de l'unité) de cette matrice sont les polynômes

$$e_4(\lambda) = (\lambda - 1)^2 (\lambda + 2),$$
$$e_3(\lambda) = \lambda - 1.$$

Nous voyons que la matrice A se réduit à la forme normale de Jordan même sur le champ des nombres rationnels. Ses diviseurs élémentaires sont les polynômes $(\lambda - 1)^2$, $\lambda - 1$ et $\lambda + 2$, de sorte que la forme normale de Jordan de la matrice A est la matrice

$$J = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}$$

Si nous voulions calculer la matrice non dégénérée transmuant la matrice A en la matrice J, nous devrions utiliser les remarques faites à la fin du paragraphe précédent.

Enfin, en s'appuyant sur les résultats obtenus, on peut donner une *condition nécessaire et suffisante de la réductibilité d'une matrice à la forme diagonale*, qui a pour conséquence immédiate le critère suffisant de la réductibilité à la forme diagonale, démontré au § 33.

Une matrice A *d'ordre* n *à éléments dans un champ* P *est réductible à la forme diagonale si et seulement si toutes les racines du dernier fac-*

teur invariant $e_n(\lambda)$ *de la matrice caractéristique* $A - \lambda E$ *appartiennent au champ* P *et si, en outre, ces racines sont toutes simples.*

En effet, la réductibilité d'une matrice à la forme diagonale est équivalente à la réductibilité de cette matrice à une forme normale de Jordan telle que toutes les cellules de Jordan soient d'ordre unité. Autrement dit, les diviseurs élémentaires de la matrice A doivent être des polynômes du premier degré. Or, les facteurs invariants de la matrice $A - \lambda E$ étant des diviseurs du polynôme $e_n(\lambda)$, il en résulte que cette dernière condition est équivalente à ce que les diviseurs élémentaires du polynôme $e_n(\lambda)$ soient de degré unité, ce qu'il fallait démontrer.

§ 62. Polynôme minimal

Soit une matrice carrée A d'ordre n à éléments dans un champ P. Soit un polynôme de l'anneau $P[\lambda]$,

$$f(\lambda) = \alpha_0\lambda^k + \alpha_1\lambda^{k-1} + \ldots + \alpha_{k-1}\lambda + \alpha_k;$$

alors la matrice

$$f(A) = \alpha_0 A^k + \alpha_1 A^{k-1} + \ldots + \alpha_{k-1}A + \alpha_k E$$

est dite *valeur* du polynôme $f(\lambda)$ pour $\lambda = A$; il faut attirer l'attention du lecteur sur le fait que le terme indépendant de λ du polynôme $f(\lambda)$ multiplie dans l'expression de $f(A)$ la puissance nulle de la matrice A, c'est-à-dire la matrice unité E.

On vérifie aisément que pour

$$f(\lambda) = \varphi(\lambda) + \psi(\lambda)$$

et pour

$$f(\lambda) = u(\lambda)\, v(\lambda),$$

on a, respectivement,

$$f(A) = \varphi(A) + \psi(A),$$
$$f(A) = u(A)\, v(A).$$

Si la matrice A annule le polynôme $f(\lambda)$, c'est-à-dire si

$$f(A) = 0,$$

alors la matrice A est appelée *racine matricielle* ou, encore, s'il n'y a pas de danger de confusion, *racine* du polynôme $f(\lambda)$.

Toute matrice A *est une racine d'un polynôme non nul.*

En effet, on sait que les matrices carrées d'ordre n forment un espace vectoriel à n^2 dimensions sur le champ P. Il en résulte que

la famille de n^2+1 matrices

$$A^{n^2},\ A^{n^2-1},\ \ldots,\ A,\ E$$

est non libre sur le champ P, c'est-à-dire qu'il existe dans P des éléments $\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{n^2}$ ne s'annulant pas simultanément et tels que l'on ait

$$\alpha_0 A^{n^2}+\alpha_1 A^{n^2-1}+\ldots+\alpha_{n^2-1}A+\alpha_{n^2}E=0.$$

Ainsi, la matrice A est une racine du polynôme non nul de degré au plus n^2:

$$\varphi(\lambda)=\alpha_0\lambda^{n^2}+\alpha_1\lambda^{n^2-1}+\ldots+\alpha_{n^2-1}\lambda+\alpha_{n^2}.$$

La matrice A est aussi une racine de certains polynômes dont le coefficient du terme principal est l'unité; en effet, il suffit de diviser tous les coefficients d'un polynôme non nul ayant A pour racine par le coefficient du terme principal. Un polynôme à coefficient unité dans le terme principal ayant A pour racine et étant du plus petit degré possible est dit *polynôme minimal associé à une matrice A*. Notons qu'*un polynôme minimal associé à une matrice A est bien défini*, car la différence de deux polynômes de ce genre serait de degré inférieur à celui de chacun de ces polynômes, mais aurait également A pour racine.

Tout polynôme $f(\lambda)$ ayant une matrice A pour racine est divisible par le polynôme minimal $m(\lambda)$ associé à cette matrice.

En effet, soit

$$f(\lambda)=m(\lambda)\,q(\lambda)+r(\lambda),$$

où le degré de $r(\lambda)$ est inférieur à celui de $m(\lambda)$; alors

$$f(A)=m(A)\,q(A)+r(A)$$

et les égalités $f(A)=m(A)=0$ donnent: $r(A)=0$, ce qui contredit la définition du polynôme minimal.

Démontrons maintenant le théorème suivant:

Le polynôme minimal associé à une matrice A coïncide avec le dernier facteur invariant $e_n(\lambda)$ de la matrice caractéristique $A-\lambda E$.

Démonstration. Conservant les notations et utilisant les résultats du § 59, on peut écrire l'égalité

$$(-1)^n\,|A-\lambda E|=d_{n-1}(\lambda)\,e_n(\lambda). \tag{1}$$

Il en résulte en particulier que les polynômes $e_n(\lambda)$ et $d_{n-1}(\lambda)$ sont non nuls. Ensuite, désignons par $B(\lambda)$ la matrice adjointe de la matrice $A-\lambda E$ (cf. § 14):

$$B(\lambda)=(A-\lambda E)^*.$$

L'égalité (3) du § 14 donne

$$(A-\lambda E) B(\lambda)=|A-\lambda E| E. \tag{2}$$

D'autre part, les éléments de la matrice $B(\lambda)$ étant les mineurs d'ordre $n-1$ de la matrice $A-\lambda E$, munis des signes plus ou moins, et le polynôme $d_{n-1}(\lambda)$ étant le plus grand commun diviseur de ces mineurs, il en découle

$$B(\lambda)=d_{n-1}(\lambda) C(\lambda) ; \tag{3}$$

en outre, *le plus grand commun diviseur des éléments de la matrice $C(\lambda)$ est l'unité.*

Les égalités (2), (3) et (1) entraînent

$$(A-\lambda E) d_{n-1}(\lambda) C(\lambda)=(-1)^{n} d_{n-1}(\lambda) e_{n}(\lambda) E.$$

On peut simplifier cette égalité en divisant par le facteur non nul $d_{n-1}(\lambda)$; en effet, ceci découle de la remarque générale suivante: soient un polynôme non nul $\varphi(\lambda)$ et une λ-matrice non nulle $D(\lambda)= (d_{ij}(\lambda))$; en outre, soit $d_{st}(\lambda) \neq 0$, alors l'élément d'indices (s, t) de la matrice $\varphi(\lambda) D(\lambda)$ est le polynôme non nul $\varphi(\lambda) d_{st}(\lambda)$. Ainsi, on a

$$(A-\lambda E) C(\lambda)=(-1)^{n} e_{n}(\lambda) E,$$

d'où

$$e_{n}(\lambda) E=(\lambda E-A)[(-1)^{n+1} C(\lambda)]. \tag{4}$$

Cette formule montre que le reste de la division « à gauche » de la λ-matrice dans le premier membre par la matrice $\lambda E-A$ est la matrice nulle. Or, du lemme démontré à la fin du § 60, il vient que le reste en question est égal à la matrice $e_n(A) E = e_n(A)$. En effet, la matrice $e_n(\lambda) E$ peut être récrite sous forme d'un λ-polynôme matriciel dont les coefficients sont des matrices scalaires qui commutent avec la matrice A. Ainsi, on a

$$e_{n}(A)=0,$$

c'est-à-dire *le polynôme $e_n(\lambda)$ est, effectivement, annulé par la matrice A.*

Il en résulte que le polynôme $e_n(\lambda)$ est divisible par le polynôme minimal $m(\lambda)$ associé à la matrice A,

$$e_{n}(\lambda)=m(\lambda) q(\lambda). \tag{5}$$

Il est clair que *le coefficient du terme principal du polynôme $q(\lambda)$ est l'unité.*

Vu que $m(A)=0$, on obtient, utilisant de nouveau le lemme du § 60, que le reste de la division à gauche de la λ-matrice $m(\lambda) E$

par le binôme $\lambda E - A$ est la matrice nulle, c'est-à-dire que

$$m(\lambda) E = (\lambda E - A) Q(\lambda). \qquad (6)$$

Les égalités (5), (4) et (6) conduisent à la formule

$$(\lambda E - A)[(-1)^{n+1} C(\lambda)] = (\lambda E - A)[Q(\lambda) q(\lambda)].$$

On peut diviser les deux membres de cette formule par le facteur commun $\lambda E - A$, vu que le coefficient E du terme principal du λ-polynôme matriciel $\lambda E - A$ est une matrice non dégénérée. On obtient

$$C(\lambda) = (-1)^{n+1} Q(\lambda) q(\lambda).$$

Or, rappelons que le plus grand commun diviseur des éléments de la matrice $C(\lambda)$ est l'unité. Ceci entraîne que le polynôme $q(\lambda)$ doit être de degré nul et, le coefficient de son terme principal étant l'unité, on a $q(\lambda) = 1$. Par conséquent, vu (5), on a la formule

$$e_n(\lambda) = m(\lambda),$$

ce qu'il fallait démontrer.

Le polynôme caractéristique de la matrice A étant, en vertu de la formule (1), divisible par le polynôme $e_n(\lambda)$, il résulte du théorème que nous venons de démontrer le théorème suivant :

Théorème de Hamilton-Cayley. *Toute matrice est une racine de son polynôme caractéristique.*

Polynôme minimal d'une application linéaire. Démontrons d'abord la proposition :

Soient deux matrices semblables A et B et un polynôme $f(\lambda)$ ayant A pour racine ; alors la matrice B est aussi une racine de $f(\lambda)$.

En effet, soit

$$B = C^{-1}AC.$$

Si

$$f(\lambda) = \alpha_0\lambda^k + \alpha_1\lambda^{k-1} + \ldots + \alpha_{k-1}\lambda + \alpha_k,$$

alors

$$\alpha_0 A^k + \alpha_1 A^{k-1} + \ldots + \alpha_{k-1}A + \alpha_k E = 0.$$

Transmuant les deux membres de cette égalité par la matrice C, il vient :

$$\begin{aligned} C^{-1}(\alpha_0 A^k + \alpha_1 A^{k-1} + \ldots + \alpha_{k-1}A + \alpha_k E)\, C = \\ = \alpha_0 (C^{-1}AC)^k + \alpha_1 (C^{-1}AC)^{k-1} + \ldots + \alpha_{k-1}(C^{-1}AC) + \alpha_k E = \\ = \alpha_0 B^k + \alpha_1 B^{k-1} + \ldots + \alpha_{k-1}B + \alpha_k E = 0, \end{aligned}$$

c'est-à-dire $f(B) = 0$.

Il en découle que *les matrices semblables possèdent le même polynôme minimal.*

Soit maintenant φ une application linéaire dans un espace vectoriel à n dimensions sur un champ P. Cette application rapportée à des bases différentes de l'espace donne des matrices semblables. Le polynôme minimal de ces matrices semblables est dit *polynôme minimal de l'application linéaire* φ.

Utilisant les opérations sur les applications linéaires introduites au § 32, on peut définir la notion de *valeur* d'un polynôme

$$f(\lambda)=\alpha_0\lambda^k+\alpha_1\lambda^{k-1}+\ldots+\alpha_{k-1}\lambda+\alpha_k$$

de l'anneau $P[\lambda]$ pour $\lambda=\varphi$, φ étant une application linéaire; en effet, cette valeur est l'application linéaire

$$f(\varphi)=\alpha_0\varphi^k+\alpha_1\varphi^{k-1}+\ldots+\alpha_{k-1}\varphi+\alpha_k\varepsilon,$$

où ε est l'application identique.

Ensuite, nous dirons que le polynôme $f(\lambda)$ *est annulé* par une application linéaire φ, si

$$f(\varphi)=\omega,$$

où ω est l'application nulle.

Vu la relation entre les opérations sur les applications linéaires et sur les matrices, le lecteur n'aura pas de difficulté à démontrer que *le polynôme minimal d'une application linéaire* φ *coïncide avec le polynôme (bien défini) à coefficient unité du terme principal annulé par l'application linéaire* φ *et étant de degré minimal.* Ceci étant, les résultats obtenus ci-dessus et, en particulier, le théorème de Hamilton-Cayley peuvent être énoncés autrement, en langage des applications linéaires.

Chapitre XIV | **GROUPES**

§ 63. Définition et exemples de groupes

Les anneaux et les champs dont le rôle était si important dans les chapitres précédents sont des ensembles munis de deux opérations algébriques indépendantes, de l'addition et de la multiplication. Toutefois, on rencontre souvent dans différentes branches des mathématiques et dans leurs applications des ensembles sur lesquels n'est définie qu'une seule opération algébrique. Ainsi, notons, en nous bornant pour le moment à des exemples déjà donnés dans le livre, que l'ensemble des substitutions de degré n n'était muni que d'une opération algébrique, à savoir de la multiplication (cf. § 3). D'autre part, la définition d'un espace vectoriel (cf. § 8) ne contient que l'addition des vecteurs tandis que la multiplication des vecteurs n'a pas été définie (notons que la multiplication d'un vecteur par un scalaire ne satisfait pas à la définition d'une opération algébrique donnée au § 44).

Parmi les ensembles à une opération algébrique les groupes sont les plus importants. Cette notion trouve un champ d'applications très vaste et est devenue l'objet d'étude d'une branche indépendante des mathématiques, dite théorie des groupes. Ce chapitre doit être considéré comme une introduction à cette théorie ; il contient quelques faits élémentaires sur les groupes que tout mathématicien est tenu de connaître ; le chapitre sera terminé par la démonstration d'un théorème qui est moins élémentaire.

Convenons, selon l'usage adopté par la théorie générale des groupes, d'appeler *multiplication* l'opération algébrique en question et d'user des notations correspondantes. Rappelons (cf. § 44) qu'*une opération algébrique interne sur un ensemble est supposée réalisable et bien définie*, c'est-à-dire pour tout couple d'éléments a et b de l'ensemble considéré le produit ab existe et est un élément bien défini de l'ensemble en question.

On appelle *groupe* un ensemble G muni d'une opération algébrique interne qui est associative (mais pas nécessairement commutative), en outre, cette opération doit être inversible.

L'opération algébrique définie sur G pouvant être non commutative, il faut préciser ce qu'on entend par opération inverse ; cela

signifie que pour tout couple d'éléments a et b de G il existe dans G un élément x *bien défini* et un élément y *bien défini* tels que l'on ait

$$ax = b, \qquad ya = b.$$

Un groupe G composé d'un nombre fini d'éléments est dit *groupe fini* et on appelle *ordre* du groupe G le nombre de ses éléments. L'opération définie sur le groupe G étant commutative, G est dit *commutatif* ou *abélien.*

Indiquons quelques conséquences simples de la définition d'un groupe. En s'appuyant sur les raisonnements du § 44, on peut affirmer que l'associativité permet de définir d'une manière unique *le produit d'un nombre quelconque mais fini d'éléments d'un groupe*, l'ordre des facteurs devant être bien défini en raison de la non-commutativité éventuelle de l'opération dont le groupe est muni.

Passons aux conséquences découlant de l'existence de l'opération inverse.

Soit a un élément du groupe G. La définition d'un groupe entraîne l'existence dans G d'un élément e_a bien défini tel que l'on ait : $ae_a = a$; cet élément tient pour a le rôle d'unité à droite. Soit b un autre élément du groupe G et soit y un élément de G tel que l'égalité $ya = b$ soit vérifiée (l'existence d'un tel élément y résulte de la définition d'un groupe) ; alors on a

$$b = ya = y\,(ae_a) = (ya)\,e_a = be_a.$$

Aussi, l'élément e_a joue le rôle d'unité à droite non seulement pour a, mais pour tout élément de G ; pour cette raison nous le noterons e'. L'opération inverse étant bien définie, l'élément e' est unique.

De la même manière on peut démontrer l'existence et l'unicité d'un élément e'' de G tel que l'égalité $e''a = a$ soit vérifiée pour tout a de G. En réalité, les éléments e' et e'' coïncident, car les égalités $e''e' = e''$ et $e''e' = e'$ entraînent : $e'' = e'$. Ceci démontre que *dans tout groupe G il existe un élément e bien défini tel que l'on ait pour tout a de G les égalités*

$$ae = ea = a.$$

Cet élément, noté par le symbole 1, est appelé *élément unité* du groupe G.

Puis, pour tout élément a de G, il résulte de la définition de groupes l'existence et l'unicité d'un élément a' et d'un élément a'' tels que l'on ait

$$aa' = 1, \quad a''a = 1.$$

En réalité, les éléments a' et a'' coïncident ; en effet, les égalités

$$a''aa' = a''\,(aa') = a'' \cdot 1 = a'',$$
$$a''aa' = (a''a)\,a' = 1 \cdot a' = a'$$

entraînent : $a'' = a'$. Cet élément, noté a^{-1}, est dit *inverse* de l'élément a, c'est-à-dire

$$aa^{-1} = a^{-1}a = 1.$$

Ainsi, *tout élément d'un groupe possède un élément inverse bien défini*.

Il résulte des dernières égalités que l'élément inverse de a^{-1} est l'élément a. Il est facile ensuite de vérifier que l'élément inverse du produit d'un certain nombre d'éléments est le produit des éléments inverses ordonnés dans le sens contraire :

$$(a_1a_2 \ldots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \ldots a_2^{-1}a_1^{-1}.$$

Enfin, l'inverse de l'unité est encore l'unité.

Pour vérifier si un ensemble muni d'une opération est un groupe, on doit démontrer l'existence de l'opération inverse ; cette vérification devient beaucoup plus aisée si, au lieu de ceci, on montre l'existence d'une unité et d'un élément inverse seulement d'un côté (par exemple, à droite) sans vérifier leur unicité. Ceci devient possible grâce au *théorème* :

Soit un ensemble G muni d'une opération interne associative ; G est un groupe s'il existe dans G au moins un élément e vérifiant pour tout a de G l'égalité

$$ae = a$$

et si, de plus, il existe, parmi ces éléments unités à droite e, au moins un élément e_0 tel que tout élément a de G possède un élément inverse à droite, soit a^{-1}, qui vérifie l'égalité :

$$aa^{-1} = e_0.$$

Démonstration. Soit a^{-1} l'un des éléments inverses à droite de a. Alors on a

$$aa^{-1} = e_0 = e_0e_0 = e_0aa^{-1},$$

c'est-à-dire $aa^{-1} = e_0aa^{-1}$. Multipliant à droite les deux membres de cette égalité par un des éléments inverses à droite de a^{-1}, il vient : $ae_0 = e_0ae_0$, d'où l'on a : $a = e_0a$, e_0 étant une unité à droite dans G. Aussi, l'élément e_0 est également une unité à gauche dans G. Soient maintenant e_1 et e_2 respectivement une unité à droite et une unité à gauche ; alors les égalités

$$e_2e_1 = e_1 \quad \text{et} \quad e_2e_1 = e_2$$

entraînent : $e_1 = e_2$, autrement dit, toute unité à droite est une unité à gauche. Ceci démontre l'existence et l'unicité de l'élément unité dans l'ensemble G ; conformément à la notation introduite ci-dessus, nous désignerons cet élément par 1.

Puis, on a

$$a^{-1} = a^{-1} \cdot 1 = a^{-1}aa^{-1},$$

c'est-à-dire $a^{-1} = a^{-1}aa^{-1}$, où a^{-1} est un des éléments inverses à droite de a. Multipliant à droite les deux membres de la dernière égalité par un des éléments inverses à droite de a^{-1}, il vient: $1 = a^{-1}a$, c'est-à-dire l'élément a^{-1} est en même temps un élément inverse à gauche de a. Soient maintenant a_1^{-1} et a_2^{-1} des éléments inverses de a respectivement à droite et à gauche; alors les égalités

$$a_2^{-1}aa_1^{-1} = (a_2^{-1}a)\,a_1^{-1} = a_1^{-1},$$
$$a_2^{-1}aa_1^{-1} = a_2^{-1}\,(aa_1^{-1}) = a_2^{-1}$$

entraînent: $a_1^{-1} = a_2^{-1}$, ce qui prouve l'existence et l'unicité de l'élément inverse a^{-1} de tout élément a de G.

A présent, il est facile de montrer que l'ensemble G est un groupe. En effet, les équations $ax = b$ et $ya = b$ ont pour solutions les éléments

$$x = a^{-1}b, \qquad y = ba^{-1}.$$

L'unicité de ces solutions résulte des raisonnements suivants: soient x_1 et x_2 tels que $ax_1 = ax_2$; multipliant à gauche les deux membres de cette égalité par a^{-1}, nous obtenons $x_1 = x_2$. Le théorème est démontré.

Nous avons déjà rencontré plusieurs fois la notion d'isomorphisme : on a parlé d'isomorphisme des anneaux, des espaces vectoriels, des espaces euclidiens. Cette notion, qui peut être aussi définie pour les groupes, joue dans la théorie des groupes un rôle aussi important que dans celle des anneaux. Deux groupes G et G' sont dits *isomorphes* s'il existe une application bijective de G sur G' telle que pour tout couple d'éléments a et b de G ayant pour images respectivement a' et b' de G', l'image du produit ab soit le produit $a'b'$. Tout comme dans le § 46 pour l'élément nul et l'élément inverse d'un anneau, on peut montrer que l'image de l'unité d'un groupe G par isomorphisme est l'unité du groupe G', de même que pour tout élément a de G, dont l'image est a' de G', l'image de a^{-1} par isomorphisme est l'élément a'^{-1}.

Avant de passer à des *exemples*, remarquons que si un groupe est noté additivement, alors l'opération de groupe est l'*addition*, l'élément unité du groupe, noté 0, s'appelle *élément nul*, et, au lieu de l'inverse d'un élément a du groupe, on aura l'*élément opposé*, noté $-a$.

Comme premier exemple de groupes, citons les *anneaux* (*et, en particulier, les champs*) *qui sont même des groupes abéliens par rapport à l'addition*; c'est ce qu'on appelle le *groupe additif d'un anneau*. Cette remarque permet de citer un grand nombre de groupes concrets et, notamment, le groupe additif des nombres entiers, celui des nombres pairs, les groupes additifs des nombres rationnels, réels, complexes, etc. Notons que *les groupes additifs des nombres entiers*

et des nombres pairs sont isomorphes, bien que le second groupe soit un sous-ensemble du premier: l'application faisant correspondre à tout nombre entier k le nombre pair $2k$ est bijective et, comme il est facile de le vérifier, c'est même un isomorphisme entre le groupe des nombres entiers et le groupe des nombres pairs.

Par contre, aucun anneau n'est un groupe par rapport à la multiplication, car l'opération inverse qu'est la division n'est pas toujours réalisable. La situation ne change pas lorsqu'on passe d'un anneau à un champ, car dans un champ on ne peut pas diviser par le zéro. Néanmoins, considérons les éléments non nuls d'un champ. Un champ n'ayant pas de diviseurs de zéro, c'est-à-dire le produit de tout couple d'éléments non nuls étant un élément non nul, la multiplication est une opération algébrique associative et commutative sur l'ensemble des éléments non nuls du champ; de plus, l'opération inverse qu'est la division existe pour tout élément de cet ensemble. Ainsi, *l'ensemble des éléments non nuls d'un champ est un groupe abélien*; ce groupe est dit *groupe multiplicatif du champ*. Les groupes multiplicatifs des nombres rationnels, réels et complexes sont des exemples de tels groupes.

Il est clair que l'ensemble des nombres réels positifs est un groupe multiplicatif. *Ce groupe est isomorphe au groupe additif des nombres réels*; en effet, faisant correspondre à tout nombre positif a le nombre réel $\ln a$, nous obtenons une application bijective du premier groupe sur le second, qui, vu l'égalité

$$\ln(ab) = \ln a + \ln b,$$

est un isomorphisme.

Ensuite, fixons dans le champ des nombres complexes l'ensemble des racines $n^{\text{èmes}}$ de l'unité. On a montré au § 19 que le produit de deux racines $n^{\text{èmes}}$ de l'unité ainsi que le nombre inverse d'une telle racine sont encore des racines $n^{\text{èmes}}$ de l'unité. L'unité étant manifestement un élément de l'ensemble en question et la multiplication des nombres complexes étant associative et commutative, on arrive à la conclusion que *les racines $n^{\text{èmes}}$ de l'unité forment un groupe abélien noté multiplicativement*; *en outre, ce groupe est fini d'ordre n*. Ainsi, *pour tout nombre naturel n il existe des groupes finis d'ordre n.*

Le groupe multiplicatif des racines $n^{\text{èmes}}$ de l'unité est isomorphe au groupe additif de l'anneau Z_n construit au § 45. En effet, soit ε une racine primitive $n^{\text{ème}}$ de l'unité; alors les éléments du premier groupe sont de la forme ε^k avec $k = 0, 1, \ldots, n-1$. Faisant correspondre à l'élément ε^k l'élément C_k de l'anneau Z_n, c'est-à-dire la classe des nombres entiers qui, divisés par n, donnent k pour reste, nous obtenons une application isomorphe des deux groupes en question, car si $0 \leqslant k \leqslant n-1$, $0 \leqslant l \leqslant n-1$, $k + l =$

$= nq + r$ avec $0 \leqslant r \leqslant n-1$, $0 \leqslant q \leqslant 1$, alors $\varepsilon^k \cdot \varepsilon^l = \varepsilon^r$ et $C_k + C_l = C_r$.

Il est temps d'indiquer des ensembles numériques qui ne sont pas groupes. Ainsi, l'ensemble des nombres entiers n'est pas un groupe par rapport à la multiplication, l'ensemble des nombres réels positifs n'est pas un groupe par rapport à l'addition, l'ensemble des nombres impairs n'est pas un groupe par rapport à l'addition, l'ensemble des nombres réels négatifs n'est pas un groupe par rapport à la multiplication. La vérification de ces propositions ne présente pas de difficulté.

Bien entendu, les groupes numériques considérés ci-dessus sont des groupes abéliens. Les espaces vectoriels fournissent des exemples de groupes abéliens dont les éléments ne sont plus les nombres; il découle de la définition des espaces vectoriels (cf. §§ 29, 47) que *tout espace vectoriel sur un champ P est un groupe abélien par rapport à l'addition des vecteurs.*

Passons à des *exemples de groupes non commutatifs.*

L'ensemble des matrices d'ordre n sur un champ P n'est pas un groupe par rapport à la multiplication, car la condition d'existence de l'élément inverse n'est pas vérifiée pour toute matrice. Toutefois, en nous bornant à l'ensemble des matrices non dégénérées, nous obtenons un groupe. En effet, le produit de deux matrices non dégénérées est, comme on le sait, une matrice non dégénérée, la matrice unité est non dégénérée, toute matrice non dégénérée possède une matrice inverse qui est encore non dégénérée, et, enfin, la loi d'associativité étant valable pour toutes les matrices, elle l'est, en particulier, pour les matrices non dégénérées. Donc, on peut parler du *groupe des matrices non dégénérées d'ordre n* sur un champ P avec la multiplication des matrices pour opération de groupe; ce groupe pour $n \geqslant 2$ n'est pas commutatif.

La multiplication des substitutions de degré n, définie au § 3, conduit à un groupe fini non commutatif très important. On sait que la multiplication dans l'ensemble des substitutions de degré n est une opération algébrique associative (quoique non commutative pour $n \geqslant 3$), que la substitution identique E joue le rôle d'unité pour cette multiplication et que toute substitution de degré n est inversible. Ainsi, *l'ensemble des substitutions de degré n est un groupe multiplicatif fini d'ordre $n!$.* Ce groupe est dit *groupe symétrique de degré n*; il n'est pas commutatif pour $n \geqslant 3$.

Au lieu de prendre toutes les substitutions de degré n, considérons à présent seulement les substitutions *paires* qui sont, comme on le sait, au nombre de $\frac{1}{2}n!$. Utilisant le théorème démontré au § 3 qui dit que la parité d'une substitution coïncide avec la parité du nombre de ses transpositions, nous arrivons à la conclusion que

le produit de deux substitutions paires est encore une substitution paire; en effet, nous obtenons la représentation du produit AB de deux substitutions A et B sous la forme d'un produit d'un nombre pair de transpositions en décomposant A et B en produits de transpositions et en les écrivant l'une après l'autre. Puis, on sait que la multiplication des substitutions est associative et que la substitution identique est paire. Enfin, une substitution A étant paire, il en est de même de A^{-1}, ce qui s'ensuit, par exemple, du fait que l'on obtient A^{-1} en échangeant les lignes de A, ce qui signifie que le nombre des inversions dans A et dans A^{-1} est le même. Ainsi, *l'ensemble des substitutions paires de degré n est un groupe multiplicatif fini d'ordre* $\frac{1}{2}n!$. Ce groupe est dit *groupe alterné de degré n*; il est facile de vérifier que pour $n \geqslant 4$ il n'est pas commutatif; pour $n = 3$ ce groupe est commutatif.

Les groupes symétriques et alternés jouent un rôle très important dans la théorie générale des groupes finis, de même que dans la théorie de Galois. Remarquons qu'il est impossible de construire, par analogie aux groupes alternés, un groupe multiplicatif de substitutions impaires, le produit de deux substitutions impaires étant une substitution paire.

Un grand nombre d'exemples de groupes est fourni par différentes branches de la géométrie. Indiquons un simple exemple de ce genre: l'ensemble de toutes les rotations d'une boule autour de son centre est un groupe non commutatif, à condition que l'on définisse le produit de deux rotations comme une rotation correspondant à l'application successive des deux rotations en question.

§ 64. Sous-groupes

Un sous-ensemble A d'un groupe G est dit *sous-groupe* de G si A est un groupe par rapport à l'opération de groupe définie sur G.

Pour vérifier qu'un sous-ensemble A d'un groupe G est un sous-groupe de G, il suffit que les conditions suivantes soient satisfaites: 1) le produit de tout couple d'éléments de A est un élément de A; 2) l'inverse de tout élément de A est encore un élément de A. En effet, la loi d'associativité étant valable pour le groupe G, elle l'est aussi pour les éléments de A; en outre, les conditions 1) et 2) garantissent l'appartenance à A de l'unité du groupe G.

Plusieurs groupes indiqués au paragraphe précédent sont des sous-groupes d'autres groupes également cités dans ce paragraphe. Aussi, le groupe additif des nombres pairs est un sous-groupe du groupe additif des nombres entiers, tandis que ce dernier est un sous-groupe du groupe additif des nombres rationnels. Tous ces groupes, ainsi que tous les groupes additifs de nombres, sont des

sous-groupes du groupe additif des nombres complexes. Le groupe multiplicatif des nombres réels positifs est un sous-groupe du groupe multiplicatif des nombres réels non nuls. Le groupe alterné de degré n est un sous-groupe du groupe symétrique de degré n.

Soulignons qu'un sous-ensemble A d'un groupe G, en vertu de la définition, n'est un sous-groupe de G que lorsque A est un groupe *par rapport à l'opération de groupe, définie sur G*. Cette condition est essentielle. Aussi, le groupe multiplicatif des nombres réels positifs n'est pas un sous-groupe du groupe additif des nombres réels bien que le premier soit un sous-ensemble du second.

Soient A et B deux sous-groupes d'un groupe G; alors leur intersection $A \cap B$, c'est-à-dire l'ensemble des éléments de G, appartenant simultanément à A et à B, est encore un sous-groupe de G.

En effet, soient x et y deux éléments de l'intersection $A \cap B$; alors x et y, de même que leur produit xy et l'élément inverse x^{-1}, appartiennent au sous-groupe A. Les mêmes raisonnements donnent que les éléments xy et x^{-1} appartiennent au sous-groupe B, de sorte que ces éléments appartiennent à l'intersection $A \cap B$.

Il est facile de voir que le résultat obtenu est vrai non seulement pour deux sous-groupes, mais aussi pour un nombre quelconque, fini ou infini, de sous-groupes.

Le sous-ensemble d'un groupe G, composé du seul élément 1, est manifestement un sous-groupe du groupe G; ce sous-groupe, qui appartient à tout sous-groupe de G, est appelé *sous-groupe unité* du groupe G. D'autre part, le groupe G est l'un de ses sous-groupes.

Un exemple de sous-groupes très intéressant est fourni par les *sous-groupes* dits *cycliques*. D'abord introduisons la notion de *puissance* d'un élément a d'un groupe G. n étant un nombre naturel, on appelle *puissance $n^{\text{ème}}$* d'un élément a et on le note a^n le produit de n facteurs égaux à a. On peut définir les *puissances d'exposants négatifs* d'un élément a d'un groupe G soit comme éléments inverses des puissances positives, soit comme les produits de facteurs égaux à l'élément a^{-1}. En réalité, ces deux définitions sont équivalentes, c'est-à-dire

$$(a^n)^{-1} = (a^{-1})^n, \qquad n > 0. \tag{1}$$

Pour le démontrer, il suffit de former le produit de $2n$ facteurs, dont n premiers sont égaux à a et les autres à a^{-1}, puis de simplifier. L'élément coïncidant avec les deux membres de (1) sera noté a^{-n}. Enfin, convenons que la *puissance d'exposant nul* a^0 de tout élément a de G soit l'élément unité.

Remarquons que, l'opération de groupe sur G étant l'addition, il faut, au lieu des puissances d'un élément a de G, parler des *multiples* de a, notés ka.

On vérifie facilement pour tout élément a d'un groupe G et pour tous les entiers m et n, positifs, négatifs ou nuls, les égalités :

$$a^n \cdot a^m = a^m \cdot a^n = a^{n+m}, \tag{2}$$

$$(a^n)^m = a^{nm}. \tag{3}$$

Désignons par $\{a\}$ le sous-ensemble du groupe G, composé de puissances de l'élément a ; bien entendu, ce sous-ensemble contient l'élément a, en tant que sa première puissance. *Le sous-ensemble* $\{a\}$ *est un sous-groupe du groupe* G ; en effet, vu (2), le produit d'éléments de $\{a\}$ est encore élément de $\{a\}$, puis l'élément unité, égal à a^0, appartient à $\{a\}$; et, enfin, un élément appartenant à $\{a\}$, il en est de même de son inverse, vu l'égalité

$$(a^n)^{-1} = a^{-n}$$

résultant de (3).

Le sous-groupe $\{a\}$ s'appelle *sous-groupe cyclique du groupe* G *engendré par l'élément* a. L'égalité (2) montre que ce sous-groupe est toujours commutatif, même si le groupe G ne l'est pas.

Notons que nous n'avons pas affirmé ci-dessus que les puissances d'un élément a étaient des éléments distincts du groupe G. S'il en est ainsi, l'élément a est dit *élément d'ordre infini*. Cependant, supposons qu'il existe parmi les puissances d'un élément a celles qui coïncident, soit, par exemple, $a^k = a^l$ avec $k \neq l$; cette situation a toujours lieu si le groupe G est fini, mais peut aussi se rencontrer dans le cas de groupes infinis. Si $k > l$, alors

$$a^{k-l} = 1,$$

c'est-à-dire il existe des puissances *positives* de l'élément a égales à l'unité. Soit n le plus petit exposant entier positif tel que la puissance correspondante de a soit l'unité, c'est-à-dire

1) $a^n = 1, \quad n > 0,$

2) si $a^k = 1, \quad k > 0$, alors $k \geqslant n$.

Dans ce cas on dit que l'élément a est un *élément d'ordre fini*, à savoir un élément *d'ordre* n.

Un élément a étant d'ordre fini n, les éléments

$$1,\ a,\ a^2,\ \ldots,\ a^{n-1} \tag{4}$$

sont tous distincts, comme il est facile de le vérifier. *Toute puissance, positive ou négative, de l'élément* a *coïncide avec l'un des éléments* (4). En effet, soit k un nombre entier ; alors, divisant k par n, on obtient

$$k = nq + r, \quad 0 \leqslant r < n,$$

de sorte que, vu (2) et (3), on a

$$a^k = (a^n)^q \cdot a^r = a^r. \tag{5}$$

Il en résulte que, *un élément a étant d'ordre fini n et* $a^k = 1$, *l'entier k doit être divisible par n.* D'autre part, vu l'égalité

$$-1 = n(-1) + (n-1),$$

on a *pour un élément a d'ordre fini n l'égalité*

$$a^{-1} = a^{n-1}.$$

La famille (4) étant composée de n éléments, il découle des résultats obtenus que, *l'élément a étant d'ordre fini, son ordre n coïncide avec l'ordre du sous-groupe cyclique* $\{a\}$, *c'est-à-dire avec le nombre des éléments de* $\{a\}$.

Enfin, notons que tout groupe n'a qu'un seul élément d'ordre un, à savoir l'élément unité. Le sous-groupe cyclique $\{1\}$ coïncide manifestement avec le sous-groupe unité.

Groupes cycliques. Un groupe G est dit *cyclique* s'il est composé de puissances d'un de ses éléments a, c'est-à-dire si G coïncide avec l'un de ses sous-groupes cycliques $\{a\}$; l'élément a est dit *générateur* du groupe G. Il est clair que tout groupe cyclique est abélien.

Le groupe additif des nombres entiers est un exemple de groupes cycliques infinis; en effet, tout nombre entier est un multiple du nombre 1, c'est-à-dire ce nombre est un générateur du groupe en question; on pourrait également prendre pour générateur le nombre — 1.

Le groupe multiplicatif des racines $n^{\text{èmes}}$ *de l'unité fournit un exemple de groupes cycliques finis d'ordre n*; en effet, on a montré au § 19 que toutes ces racines sont les puissances de l'une d'elles, à savoir d'une racine primitive.

Le théorème suivant montre que ces exemples épuisent essentiellement l'ensemble des groupes cycliques:

Tous les groupes cycliques infinis sont isomorphes, de même que sont isomorphes tous les groupes cycliques finis d'ordre n donné.

En effet, on établit une application bijective d'un groupe cyclique infini de générateur a sur le groupe additif des nombres entiers, en faisant correspondre à tout élément a^k le nombre entier k; cette application est isomorphe, car, d'après (2), la multiplication des puissances de a conduit à l'addition des exposants correspondants. Soit maintenant un groupe cyclique fini G d'ordre n ayant pour générateur l'élément a; désignant par ε une racine primitive $n^{\text{ème}}$ de l'unité, faisons correspondre à tout élément a^k de G le nombre ε^k, $0 \leqslant k < n$. C'est une application bijective du groupe G sur le groupe multiplicatif des racines $n^{\text{èmes}}$ de l'unité; il résulte de (2) et (5) que cette application est un isomorphisme.

Ce théorème nous permet de parler du *groupe cyclique infini* ou *du groupe cyclique fini d'ordre n.*

Démontrons maintenant le théorème suivant.

Tout sous-groupe d'un groupe cyclique est, lui-même, cyclique.

En effet, soit $G = \{a\}$ un groupe cyclique, fini ou infini, de générateur a, et soit A un sous-groupe du groupe G. On peut supposer que A ne soit pas le sous-groupe unité, sinon il n'y aurait rien à démontrer. Soit k, $k > 0$, le plus petit exposant entier tel que a^k appartienne à A; une telle puissance a^k existe toujours, car si A contient un élément a^{-s}, $s > 0$, différent de l'unité, alors A contient également l'élément inverse a^s. Admettons que A contienne un élément a^l, $l \neq 0$, tel que l ne soit pas divisible par k. Alors, notant par d le plus grand commun diviseur des entiers k et l, $d > 0$, il existe des nombres entiers u et v tels que l'on ait

$$ku + lv = d,$$

de sorte que le sous-groupe A doit contenir l'élément

$$(a^k)^u \cdot (a^l)^v = a^d;$$

or, étant donné nos hypothèses $d < k$, ceci est en contradiction avec le choix de a^k. Cette contradiction démontre que $A = \{a^k\}$.

Décomposition d'un groupe suivant son sous-groupe. Soient deux sous-ensembles M et N d'un groupe G; on entend par *produit MN des sous-ensembles M et N* l'ensemble des éléments de G tels qu'une représentation de ces éléments sous la forme d'un produit de deux facteurs respectivement de M et de N soit possible. L'associativité de l'opération de groupe entraîne *celle de la multiplication des sous-ensembles du groupe*,

$$(MN)P = M(NP).$$

Evidemment, l'un des sous-ensembles M et N peut être composé d'un seul élément a. Dans ce cas nous obtenons le *produit aN d'un élément par un ensemble ou bien le produit Ma d'un ensemble par un élément.*

Soit A un sous-groupe du groupe G; x étant un élément de G, on appelle le produit xA *classe d'équivalence à gauche du groupe G suivant le sous-groupe A* (ou, encore, modulo A), *engendrée par l'élément x*. Il est clair que *l'élément x appartient à la classe xA*, car le sous-groupe A contient l'unité et $x \cdot 1 = x$.

Une classe d'équivalence à gauche est engendrée par tout élément appartenant à cette classe, autrement dit, l'élément y appartenant à une classe xA, on a

$$yA = xA. \qquad (6)$$

En effet, on peut représenter y sous la forme

$$y = xa,$$

où a est un élément du sous-groupe A. Par conséquent, on a pour tout couple d'éléments a' et a'' de A :

$$ya' = x(aa'),$$
$$xa'' = y(a^{-1}a''),$$

ce qui démontre l'égalité (6).

Il en résulte que *deux classes d'équivalence à gauche d'un groupe G modulo A soit coïncident, soit sont disjointes.* En effet, soit z un élément commun aux classes xA et yA ; alors

$$xA = zA = yA.$$

Ainsi, le groupe G se décompose en classes d'équivalence à gauche suivant un sous-groupe A, qui sont disjointes deux à deux. Cette décomposition est dite *décomposition à gauche du groupe G suivant un sous-groupe A.*

Remarquons que l'une des classes d'équivalence à gauche de cette décomposition est le sous-groupe A ; cette classe est engendrée par l'élément unité ou, plus généralement, par tout élément a de A, car

$$aA = A.$$

Bien entendu, appelant le produit *Ax classe d'équivalence à droite du groupe G modulo A, engendrée par l'élément x*, nous obtenons, de façon analogue, une *décomposition à droite du groupe G suivant un sous-groupe A.* Il est clair que si un groupe G est abélien, alors les deux décompositions, à gauche et à droite, suivant un sous-groupe de G, coïncident et l'on peut parler de la *décomposition d'un groupe abélien suivant son sous-groupe* tout court.

Aussi, la décomposition du groupe additif des nombres entiers suivant le sous-groupe des nombres entiers divisibles par k contient k classes d'équivalence distinctes, engendrées respectivement par les nombres $0, 1, \ldots, k-1$. En outre, la classe engendrée par le nombre l, $0 \leqslant l \leqslant k-1$, est composée des nombres entiers qui, divisés par k, donnent l pour reste.

Dans le cas non commutatif les décompositions à gauche et à droite d'un groupe suivant un sous-groupe peuvent être distinctes.

Considérons, par exemple, le groupe symétrique S_3 de degré 3. Il est commode d'écrire les éléments de S_3 sous forme de cycles (cf. § 3). Choisissons pour sous-groupe A le sous-groupe cyclique de l'élément (12) ; A contient la substitution identique et la substitution (12). Les autres classes d'équivalence à gauche modulo A sont respectivement la classe $(13)\cdot A$ composée des substitutions (13) et (132) et la classe $(23)\cdot A$ composée des substitutions (23) et (123). D'autre part, les classes d'équivalence à droite du groupe S_3 modulo A sont : le sous-groupe A, la classe $A\cdot(13)$ composée

des substitutions (13) et (123), et la classe $A\cdot(23)$ composée des substitutions (23) et (132). Nous constatons que dans le cas considéré la décomposition de S_3 à droite ne coïncide pas avec celle à gauche.

Dans le cas de groupes finis l'existence de la décomposition d'un groupe suivant un sous-groupe conduit au théorème important suivant:

Théorème de Lagrange. *L'ordre de tout sous-groupe d'un groupe fini est un diviseur de l'ordre du groupe.*

En effet, soit A un sous-groupe d'ordre k d'un groupe fini G d'ordre n. Considérons la décomposition à gauche du groupe G suivant le sous-groupe A. Supposons que cette décomposition contienne j classes; le nombre j s'appelle *indice* du sous-groupe A dans le groupe G. Toute classe à gauche xA contient exactement k éléments, car si

$$xa_1 = xa_2,$$

avec a_1 et a_2 éléments de A, alors $a_1 = a_2$. Par conséquent,

$$n = kj, \tag{7}$$

ce qu'il fallait démontrer.

L'ordre d'un élément coïncidant avec l'ordre du sous-groupe cyclique ayant cet élément pour générateur, il résulte du théorème de Lagrange que *l'ordre de tout élément d'un groupe fini est un diviseur de l'ordre du groupe considéré.*

Il découle également du théorème de Lagrange que *tout groupe fini ayant pour ordre un nombre premier est un groupe cyclique.* En effet, un tel groupe doit coïncider avec tout sous-groupe cyclique engendré par un élément de ce groupe différent de l'unité. Il en résulte, vu la description des groupes cycliques ci-dessus, que *pour tout nombre premier p il existe, à un isomorphisme près, un seul groupe fini d'ordre p.*

§ 65. Sous-groupes distingués, groupes-quotients, homomorphismes

Un sous-groupe A d'un groupe G est dit *sous-groupe distingué* de G (ou *sous-groupe invariant* de G) si les décompositions à gauche et à droite du groupe G suivant le sous-groupe A coïncident.

Aussi tout sous-groupe d'un groupe abélien est-il un sous-groupe distingué du groupe en question. D'autre part, quel que soit le groupe G, G et le sous-groupe unité sont des sous-groupes distingués de G; en effet, les décompositions à gauche et à droite du groupe G suivant le sous-groupe unité coïncident avec la décomposition de G en ses éléments, tandis que les décompositions à gauche et à droite du groupe G suivant G ne contiennent qu'une seule classe, à savoir le groupe G.

Indiquons des exemples moins banals de sous-groupes distingués d'un groupe non commutatif. Dans le groupe symétrique S_3 du troisième degré, le sous-groupe cyclique à générateur (123) composé de la substitution identique et des substitutions (123) et (132) est un sous-groupe distingué car les décompositions à gauche et à droite du groupe S_3 suivant le sous-groupe en question, outre ce sous-groupe, contiennent toutes les deux la même classe d'équivalence, composée des substitutions (12), (13) et (23).

Plus généralement, le sous-groupe alterné A_n de degré n du groupe symétrique S_n de degré n est un sous-groupe distingué de S_n. En effet, le groupe A_n est d'ordre $\frac{1}{2}n!$; par conséquent, toute classe d'équivalence du groupe S_n modulo A_n doit contenir exactement le même nombre d'éléments, de sorte que, outre A_n, il y a encore une seule classe d'équivalence du groupe S_n modulo A_n, à savoir l'ensemble des substitutions impaires.

Dans le groupe multiplicatif des matrices carrées non dégénérées d'ordre n à éléments dans un champ P le sous-ensemble des matrices à déterminant unité est, manifestement, un sous-groupe. De plus, ce sous-groupe est un sous-groupe distingué, car la classe d'équivalence à gauche et à droite suivant ce sous-groupe, engendrée par une matrice M, est composée par toutes les matrices dont le déterminant est égal à celui de M; en effet, il suffit de rappeler que le déterminant du produit de matrices est le produit des déterminants.

La définition d'un sous-groupe distingué donnée ci-dessus peut être énoncée sous une autre forme :

Un sous-groupe A d'un groupe G est dit sous-groupe distingué de G, si pour tout élément x de G on a l'égalité

$$xA = Ax, \tag{1}$$

c'est-à-dire si pour tout élément x de G et tout élément a de A on peut trouver des éléments a' et a'' de A tels que l'on ait

$$xa = a'x, \qquad ax = xa''. \tag{2}$$

On peut aussi indiquer d'autres définitions de sous-groupes distingués, équivalentes à la définition initiale. Aussi, appelons deux éléments a et b d'un groupe G *conjugués*, s'il existe dans G un élément x tel que l'on ait

$$b = x^{-1}ax, \tag{3}$$

ou, comme on dit, si l'élément b s'obtient en *transmuant* l'élément a par l'élément x. Il résulte de (3) l'égalité évidente :

$$a = xbx^{-1} = (x^{-1})^{-1}\,bx^{-1}.$$

Un sous-groupe A d'un groupe G est un sous-groupe distingué de G si et seulement si pour tout élément a de A le sous-groupe A contient aussi tous les éléments conjugués de a dans G.

En effet, si A est un sous-groupe distingué de G, alors, vu (2), pour un élément fixe a de A et pour tout x de G on peut trouver un élément a'' de A tel que

$$ax = xa''.$$

Il en résulte que

$$x^{-1}ax = a'',$$

c'est-à-dire tout élément conjugué de a appartient à A. Inversement, soit un sous-groupe A tel qu'il contienne, avec tout élément a, tous les éléments conjugués de a dans G; alors A contient, en particulier, l'élément

$$x^{-1}ax = a'',$$

d'où résulte la seconde égalité (2). Pour la même raison A contient aussi l'élément

$$(x^{-1})^{-1}\, ax^{-1} = xax^{-1} = a',$$

d'où la première égalité (2).

Utilisant ces résultats, il est facile de démontrer que *l'intersection de sous-groupes distingués d'un groupe G est encore un sous-groupe distingué de G.* En effet, soient A et B deux sous-groupes distingués d'un groupe G; alors, comme on l'a démontré au paragraphe précédent, l'intersection $A \cap B$ est un sous-groupe de G. Soient c un élément de $A \cap B$ et x un élément de G. Alors l'élément $x^{-1}cx$ doit appartenir à A et B, car les sous-groupes distingués A et B contiennent tous les deux l'élément c. Il en découle que l'élément $x^{-1}cx$ appartient à l'intersection $A \cap B$.

Groupe-quotient. L'importance de la notion de sous-groupe distingué est due à ce que, utilisant les classes d'équivalence d'un groupe suivant un sous-groupe distingué (vu (1), on peut ne pas faire de distinction entre les classes à gauche et celles à droite), on peut former de façon naturelle un nouveau groupe.

Notons d'abord que, A étant un sous-groupe d'un groupe G, on a

$$AA = A, \tag{4}$$

car le produit de tout couple d'éléments de A est encore un élément de A et, en même temps, multipliant tous les éléments de A par l'unité, nous obtenons le sous-groupe A.

A présent, soit A un sous-groupe distingué d'un groupe G. *Dans ce cas, le produit de deux classes d'équivalence de G modulo A* (le produit de classes étant interprété du point de vue de la multiplication

des sous-ensembles de G) *est encore une classe d'équivalence de G modulo A*. En effet, la multiplication des sous-ensembles d'un groupe étant associative, l'égalité (4) et l'égalité

$$yA = Ay$$

(cf. (1)) donnent pour tout couple d'éléments x et y du groupe G:

$$xA \cdot yA = xyAA = xyA. \tag{5}$$

La formule (5) montre que pour trouver le produit de deux classes d'équivalence du groupe G modulo A il faut fixer dans chaque classe un élément quelconque *représentant* cette classe (rappelons qu'une classe d'équivalence est engendrée par l'un quelconque de ses éléments) et prendre ensuite la classe qui contient le produit de ces représentants.

Ainsi, une opération de multiplication est définie sur l'ensemble des classes d'équivalence d'un groupe G suivant son sous-groupe distingué A. Montrons que *cette opération vérifie la définition de groupes.* En effet, l'associativité de la multiplication des classes résulte de l'associativité de la multiplication des sous-ensembles d'un groupe. Le rôle d'unité est tenu par le sous-groupe distingué A qui est une des classes d'équivalence de la décomposition de G modulo A ; en effet, vu (4) et (1), on a pour x de G:

$$xA \cdot A = xA, \qquad A \cdot xA = xAA = xA.$$

Enfin, l'inverse d'une classe xA est la classe $x^{-1}A$, car on a

$$xA \cdot x^{-1}A = 1 \cdot A = A.$$

Le groupe que nous avons construit est dit *groupe-quotient* du groupe G suivant le sous-groupe distingué A ou, encore, groupe-quotient de G par A ; il est noté G/A.

On voit que l'on peut associer à tout groupe une suite de nouveaux groupes, à savoir les groupes-quotients du groupe donné par tous ses sous-groupes distingués. En outre, il est clair que le groupe-quotient d'un groupe G suivant le sous-groupe unité est isomorphe à G.

Tout groupe-quotient G/A d'un groupe abélien G par A est abélien, car l'égalité $xy = yx$ entraîne

$$xA \cdot yA = xyA = yxA = yA \cdot xA.$$

Tout groupe-quotient G/A d'un groupe cyclique G par A est cyclique; en effet, soit g un générateur de G, $G = \{g\}$, et soit xA une classe d'équivalence; alors il existe un entier k tel que l'on ait

$$x = g^k,$$

de sorte que

$$xA = (gA)^k.$$

L'ordre de tout groupe-quotient G/A d'un groupe fini G par A est un diviseur de l'ordre du groupe G. En effet, l'ordre du groupe-quotient G/A est l'indice du sous-groupe distingué A dans le groupe G et, par conséquent, on peut se servir de l'égalité (7) du paragraphe précédent.

Donnons quelques *exemples* de groupes-quotients. On a montré dans le paragraphe précédent que le sous-groupe du groupe additif des nombres entiers, composé des nombres entiers divisibles par un nombre entier positif k, est d'indice k; par conséquent, le groupe-quotient correspondant est un groupe fini d'ordre k; en outre, il est cyclique, le groupe des nombres entiers jouissant de cette propriété.

Le groupe-quotient du groupe symétrique S_n de degré n par le sous-groupe alterné A_n de degré n est un groupe d'ordre 2; en outre, le nombre 2 étant premier, le groupe-quotient en question est cyclique (cf. la fin du paragraphe précédent).

On a donné ci-dessus la description des classes d'équivalence de la relation définie dans le groupe multiplicatif des matrices carrées non dégénérées d'ordre n à éléments dans un champ P par le sous-groupe distingué composé des matrices à déterminant unité. Il s'ensuit de cette description que le groupe-quotient correspondant est isomorphe au groupe multiplicatif des nombres non nuls du champ P.

Homomorphisme. La notion de sous-groupe distingué et celle de groupe-quotient sont très étroitement liées à la généralisation suivante de la notion d'isomorphisme.

Une application φ d'un groupe G sur un groupe G' faisant correspondre à tout élément a de G un élément $a' = a\varphi$ bien défini de G' s'appelle *application homomorphe* (ou *homomorphisme* tout court) de G sur G' si, quel que soit a' de G', il existe un élément a de G, dont a' est l'image par φ: $a' = a\varphi$, et si, de plus, pour tout couple d'éléments a et b de G on a

$$(ab)\,\varphi = a\varphi \cdot b\varphi.$$

Il est clair que l'on obtient la définition de l'isomorphisme, déjà connue, en exigeant que l'application φ soit bijective.

Soit φ un homomorphisme d'un groupe G sur un groupe G'; soient 1 et 1' respectivement les éléments unités de G et de G'. Alors on a pour tout élément a du groupe G

$$1\varphi = 1',$$
$$(a^{-1})\,\varphi = (a\varphi)^{-1}.$$

En effet, supposons que $1\varphi = e'$ et soit x' un élément de G'; alors il existe un élément x de G tel que l'on ait: $x\varphi = x'$. Il en

résulte que

$$x' = x\varphi = (x \cdot 1)\,\varphi = x\varphi \cdot 1\varphi = x' \cdot e'.$$

De manière analogue, on a

$$x' = e'x'$$

et, par conséquent, $e' = 1'$.

D'autre part, si $(a^{-1})\,\varphi = b'$, alors on a la formule

$$1' = 1\varphi = (aa^{-1})\,\varphi = a\varphi \cdot (a^{-1})\,\varphi = a\varphi \cdot b'$$

et, de la même manière, la formule

$$1' = b' \cdot a\varphi,$$

d'où $b' = (a\varphi)^{-1}$.

Appelons *noyau* d'un homomorphisme φ, appliquant un groupe G sur un groupe G', l'ensemble des éléments de G tels que leurs images dans G' par φ soient l'élément unité $1'$ de G'.

Le noyau de tout homomorphisme φ d'un groupe G sur un autre groupe est un sous-groupe distingué de G.

En effet, a et b étant deux éléments du noyau en question, c'est-à-dire les égalités

$$a\varphi = b\varphi = 1'$$

ayant lieu, on a

$$(ab)\,\varphi = a\varphi \cdot b\varphi = 1' \cdot 1' = 1',$$

autrement dit, le produit ab appartient au noyau de l'homomorphisme φ. D'autre part, si $a\varphi = 1'$, alors

$$(a^{-1})\,\varphi = (a\varphi)^{-1} = 1'^{-1} = 1',$$

c'est-à-dire a^{-1} appartient au noyau de φ. Enfin, si $a\varphi = 1'$, alors on a pour tout élément x du groupe G :

$$(x^{-1}ax)\,\varphi = (x^{-1})\,\varphi \cdot a\varphi \cdot x\varphi = (x\varphi)^{-1} \cdot 1' \cdot x\varphi = 1'.$$

Aussi, le noyau de l'homomorphisme considéré est un sous-groupe du groupe G tel que, avec tout élément a, ce sous-groupe contient tous les éléments conjugués de a ; par conséquent, le sous-groupe en question est un sous-groupe distingué.

Maintenant, soit A un sous-groupe distingué d'un groupe G. Associant à tout élément x de G la classe d'équivalence xA de G modulo A (xA est la classe qui contient x), nous obtenons une application du groupe G sur le groupe-quotient G/A. Il résulte de la multiplication définie sur le groupe G/A (cf. (5)) que cette application est un homomorphisme. Il s'appelle *homomorphisme naturel* du groupe G sur le groupe-quotient G/A. Il est clair que son noyau est le sous-groupe distingué A.

Il en résulte que *les sous-groupes distingués d'un groupe G, et seulement ces sous-groupes, sont les noyaux des homomorphismes du groupe G.* Ce résultat peut être considéré comme une nouvelle définition d'un sous-groupe distingué.

Il apparaît que les groupes, images d'un groupe G par les homomorphismes, coïncident avec les groupes-quotients de G, tandis que tous les homomorphismes du groupe G coïncident avec les homomorphismes naturels de G sur les groupes-quotients correspondants. Plus précisément, le théorème suivant est vrai :

Théorème des homomorphismes. *Soient φ un homomorphisme d'un groupe G sur un groupe G' et A le noyau de φ. Alors le groupe G' est isomorphe au groupe-quotient G/A ; de plus, il existe une application isomorphe σ de G' sur G/A telle que le produit des applications φ et σ est un homomorphisme naturel du groupe G sur le groupe-quotient G/A.*

En effet, soit x' un élément du groupe G' et soit x un élément du groupe G tel que $x\varphi = x'$. Vu que pour tout élément a du noyau A de l'homomorphisme φ l'égalité $a\varphi = 1'$ est satisfaite, on a

$$(xa)\varphi = x\varphi \cdot a\varphi = x' \cdot 1' = x',$$

c'est-à-dire x' est l'image par φ des éléments de la classe d'équivalence xA.

D'autre part, soit z un élément du groupe G tel que $z\varphi = x'$; alors

$$(x^{-1}z)\varphi = x^{-1}\varphi \cdot z\varphi = (x\varphi)^{-1} \cdot z\varphi = x'^{-1} \cdot x' = 1',$$

c'est-à-dire $x^{-1}z$ appartient au noyau A de l'homomorphisme φ. Posant $x^{-1}z = a$, il vient $z = xa$, c'est-à-dire l'élément z appartient à la classe xA. Aussi, l'ensemble des éléments du groupe G, dont l'image par l'homomorphisme φ est un élément fixe x' de G', coïncide avec la classe d'équivalence xA.

L'application σ faisant correspondre à tout élément x' de G' la classe d'équivalence de G modulo A composée des éléments du groupe G, dont l'image par φ est x', définit une application bijective du groupe G' sur le groupe G/A. L'application σ est un isomorphisme, car, vu les égalités

$$x'\sigma = xA, \qquad y'\sigma = yA,$$

c'est-à-dire les égalités

$$x\varphi = x', \quad y\varphi = y',$$

on a

$$(xy)\varphi = x\varphi \cdot y\varphi = x'y',$$

de sorte que

$$(x'y')\sigma = xyA = xA \cdot yA = x'\sigma \cdot y'\sigma.$$

Enfin, si x est un élément de G et $x\varphi = x'$, alors

$$(x\varphi)\,\sigma = x'\sigma = xA,$$

autrement dit, le produit de l'homomorphisme φ et de l'isomorphisme σ transforme réellement l'élément x en classe d'équivalence xA engendrée par x. Le théorème est démontré.

§ 66. Sommes directes de groupes abéliens

Nous voulons terminer le chapitre par la démonstration d'un théorème de la théorie des groupes qui est plus profond que les propriétés élémentaires des groupes exposées ci-dessus. Notamment, en nous appuyant sur la description des groupes cycliques donnée au § 64, nous obtiendrons au paragraphe suivant la *description complète des groupes abéliens finis.*

Comme cela est adopté dans la théorie des groupes abéliens, nous noterons additivement l'opération de groupe, c'est-à-dire on parlera de la *somme* $a + b$ de deux éléments a et b, du *sous-groupe nul*, noté 0, de *multiples* ka d'un élément a d'un groupe abélien, etc.

Ce paragraphe sera consacré à l'étude d'une construction que nous introduirons pour les groupes abéliens quoiqu'on puisse l'introduire pour un groupe quelconque, c'est-à-dire pas forcément pour un groupe commutatif. Cette construction est suggérée par les exemples suivants. Le plan, en tant qu'espace vectoriel réel à deux dimensions, est un groupe abélien par rapport à l'addition des vecteurs. Toute droite de ce plan passant par l'origine des coordonnées est un sous-groupe de ce groupe. Soient A_1 et A_2 deux droites distinctes du plan passant par l'origine; on sait que, dans ce cas, tout vecteur du plan issu de l'origine peut être représenté de façon unique comme somme de ses projections respectivement sur A_1 et A_2. De même, tout vecteur d'un espace vectoriel à trois dimensions est la somme de trois vecteurs appartenant respectivement à trois droites distinctes A_1, A_2, A_3 de l'espace et passant par l'origine, à condition que les droites A_1, A_2, A_3 ne soient pas situées dans un même plan; en outre, cette représentation est unique.

Un groupe abélien G est dit *somme directe* de ses sous-groupes $A_1, A_2, \ldots, A_k$,

$$G = A_1 \dotplus A_2 \dotplus \ldots \dotplus A_k, \tag{1}$$

si tout élément x du groupe G se décompose *uniquement* en somme des éléments $a_1, a_2, \ldots, a_k$ appartenant respectivement à A_1, $A_2, \ldots, A_k$:

$$x = a_1 + a_2 + \ldots + a_k. \tag{2}$$

L'écriture (1) s'appelle *décomposition directe* du groupe G, les sous-groupes A_i, $i = 1, 2, \ldots, k$, sont dits *termes directs* de la décomposition (1), et l'élément a_i de la décomposition (2) s'appelle *composante* de l'élément x dans le terme direct A_i de la décomposition (1), $i = 1, 2, \ldots, k$.

Soit une décomposition directe (1) *d'un groupe* G; *supposons que certains termes directs* A_i (*ou tous les* A_i) *sont, eux aussi, décomposés en sommes directes*:

$$A_i = A_{i1} + A_{i2} + \ldots + A_{ik_i}, \quad k_i \geqslant 1. \tag{3}$$

Alors le groupe G *est une somme directe de tous ses sous-groupes*

$$A_{ij}, \quad j = 1, 2, \ldots, k_i, \quad i = 1, 2, \ldots, k.$$

En effet, pour tout élément x de G il existe une écriture (2) correspondant à la décomposition (1) et pour toute composante a_i, $i = 1, 2, \ldots, k$, une écriture

$$a_i = a_{i1} + a_{i2} + \ldots + a_{ik_i} \tag{4}$$

correspondant à la décomposition directe (3) du groupe A_i. Il est clair que x est la somme des éléments a_{ij}, $j = 1, 2, \ldots, k_i$, $i = 1, 2, \ldots, k$. Cette représentation est unique; en effet, fixant une écriture quelconque de x sous forme d'une somme d'éléments, chaque élément étant pris dans son sous-groupe A_{ij}, puis additionnant les termes appartenant à un même sous-groupe A_i, $i = 1, 2, \ldots, k$, nous devons retrouver justement l'égalité (2); d'autre part, tout élément a_i possède une écriture unique de la forme (4).

On peut donner une autre forme à la définition de la somme directe. Introduisons d'abord encore une notion. Soient $B_1, B_2, \ldots, B_l$ des sous-groupes d'un groupe abélien G; désignons par $\{B_1, B_2, \ldots, B_l\}$ l'ensemble des éléments y de G tels que ces éléments possèdent *au moins une représentation* sous forme de sommes des éléments $b_1, b_2, \ldots, b_l$ appartenant respectivement à B_1, $B_2, \ldots, B_l$,

$$y = b_1 + b_2 + \ldots + b_l. \tag{5}$$

L'ensemble $\{B_1, B_2, \ldots, B_l\}$ *est un sous-groupe du groupe* G. On dit qu'il est *engendré* par les sous-groupes $B_1, B_2, \ldots, B_l$.

Pour démontrer cette proposition prenons dans $\{B_1, B_2, \ldots, B_l\}$ un élément y ayant l'écriture (5) et un élément y' ayant une écriture analogue

$$y' = b'_1 + b'_2 + \ldots + b'_l,$$

où b'_i est un élément de B_i, $i = 1, 2, \ldots, l$. Alors

$$y + y' = (b_1 + b'_1) + (b_2 + b'_2) + \ldots + (b_l + b'_l),$$
$$-y = (-b_1) + (-b_2) + \ldots + (-b_l),$$

c'est-à-dire les éléments $y+y'$ et $-y$ possèdent également une écriture du type (5) et, par conséquent, appartiennent à l'ensemble $\{B_1, B_2, \ldots, B_l\}$, ce qu'il fallait démontrer.

Le sous-groupe $\{B_1, B_2, \ldots, B_l\}$ *contient chacun des sous-groupes* B_i, $i=1, 2, \ldots, l$. En effet, tout sous-groupe du groupe G contient l'élément nul de G, de sorte que choisissant, par exemple, dans B_1 un élément b_1 et prenant l'élément nul comme composante dans les sous-groupes $B_2, \ldots, B_l$, nous obtenons pour b_1 la représentation du type (5):

$$b_1 = b_1 + 0 + \ldots + 0.$$

Pour qu'un groupe abélien G soit une somme directe de ses sous-groupes $A_1, A_2, \ldots, A_k$, *il faut et il suffit que G soit engendré par* $A_1, A_2, \ldots, A_k$,

$$G = \{A_1, A_2, \ldots, A_k\}, \tag{6}$$

et que l'intersection du sous-groupe A_i et du sous-groupe engendré par les sous-groupes $A_1, A_2, \ldots, A_{i-1}$ qui précèdent A_i, $i = 2, \ldots, k$, ne contienne que l'élément nul:

$$\{A_1, A_2, \ldots, A_{i-1}\} \cap A_i = 0, \qquad i = 2, \ldots, k. \tag{7}$$

En effet, si le groupe G possède une décomposition directe (1), alors pour *tout* élément x de G il existe une écriture (2) et, par conséquent, l'égalité (6) a lieu. La formule (7) découle de l'*unicité* de l'écriture (2) pour tout élément x de G; en effet, s'il existait un indice i tel que l'intersection $\{A_1, A_2, \ldots, A_{i-1}\} \cap A_i$ contienne un élément non nul, soit x, alors, d'une part, x, en tant qu'élément de A_i, soit a_i, aurait l'écriture: $x = a_i$ ou encore

$$x = 0 + \ldots + 0 + a_i + 0 + \ldots + 0; \tag{8}$$

d'autre part, ce même élément x, en tant qu'élément du sous-groupe $\{A_1, A_2, \ldots, A_{i-1}\}$, aurait l'écriture

$$x = a_1 + a_2 + \ldots + a_{i-1}$$

ou encore

$$x = a_1 + a_2 + \ldots + a_{i-1} + 0 + \ldots + 0. \tag{9}$$

Il est clair que (8) et (9) seraient dans ce cas deux écritures différentes de l'élément x sous la forme (2).

Inversement, soient les égalités (6) et (7). Il découle de (6) que tout élément x du groupe G possède au moins une écriture de la forme (2). Supposons qu'il y ait un élément x tel qu'il possède deux écritures (2) différentes,

$$x = a_1 + a_2 + \ldots + a_k = a'_1 + a'_2 + \ldots + a'_k. \tag{10}$$

Alors on peut trouver un indice i, $i \leqslant k$, tel que l'on ait

$$a_k = a'_k,\ a_{k-1} = a'_{k-1},\ \ldots,\ a_{i+1} = a'_{i+1}, \tag{11}$$

mais que

$$a_i \neq a'_i$$

ou encore que

$$a_i - a'_i \neq 0. \qquad (12)$$

Or, il résulte de (10) et (11) l'égalité

$$a_i - a'_i = (a'_1 - a_1) + (a'_2 - a_2) + \ldots + (a'_{i-1} - a_{i-1}),$$

qui, vu (12), est en contradiction avec l'égalité (7). Le théorème est démontré.

On peut envisager la notion de somme directe sous un autre angle. Soient k groupes abéliens quelconques $A_1, A_2, \ldots, A_k$, dont certains peuvent être isomorphes. Désignons par G l'ensemble des suites de la forme

$$(a_1, a_2, \ldots, a_k), \qquad (13)$$

composées d'éléments appartenant respectivement à $A_1, A_2, \ldots, A_k$. L'ensemble G devient un groupe abélien si l'on définit l'*addition* de suites (13) de la façon suivante:

$$(a_1, a_2, \ldots, a_k) + (a'_1, a'_2, \ldots, a'_k) = \\ = (a_1 + a'_1, a_2 + a'_2, \ldots, a_k + a'_k), \qquad (14)$$

c'est-à-dire on additionne séparément les éléments de tout groupe A_i, $i = 1, 2, \ldots, k$. En effet, l'associativité et la commutativité de l'addition ainsi obtenue découlent des propriétés correspondantes de l'addition dans chacun des groupes donnés. La suite

$$(0_1, 0_2, \ldots, 0_k)$$

est l'élément nul du groupe G; ici 0_i est l'élément nul du groupe A_i, $i = 1, 2, \ldots, k$; la suite opposée à une suite (13) est de la forme

$$(-a_1, -a_2, \ldots, -a_k).$$

Le groupe abélien G ainsi construit est dit *somme directe* des groupes $A_1, A_2, \ldots, A_k$; il est noté

$$G = A_1 + A_2 + \ldots + A_k.$$

La justification de cette appellation est la suivante. *Un groupe G qui est une somme directe, dans le sens qui vient d'être défini, des groupes abéliens $A_1, A_2, \ldots, A_k$ peut être décomposé en une somme directe (dans le sens initial) de ses sous-groupes $A'_1, A'_2, \ldots, A'_k$ de telle manière que A'_i soit isomorphe à A_i pour $i = 1, 2, \ldots, k$.*

Notamment, désignons par A'_i l'ensemble d'éléments du groupe G (les éléments de G sont les suites de la forme (13)) qui ont pour $i^{\text{ème}}$ composante les éléments a_i du groupe A_i et pour les autres composantes les éléments nuls des groupes correspondants; donc, ce sont

les suites de la forme

$$(0_1, \ldots, 0_{i-1}, a_i, 0_{i+1}, \ldots, 0_k). \tag{15}$$

La définition de l'addition (14) montre que l'ensemble A'_i est un sous-groupe du groupe G; on obtient un isomorphisme de ce sous-groupe et du groupe A_i en faisant correspondre à tout élément (15) de A'_i l'élément a_i de A_i.

Il reste à démontrer que le groupe G est une somme directe (dans le sens initial) des sous-groupes $A'_1, A'_2, \ldots, A'_k$. En effet, tout élément (13) du groupe G peut être représenté comme une somme d'éléments appartenant chacun à un sous-groupe correspondant:

$$(a_1, a_2, \ldots, a_k) = (a_1, 0_2, \ldots, 0_k) +$$
$$+ (0_1, a_2, 0_3, \ldots, 0_k) + \ldots + (0_1, 0_2, \ldots, 0_{k-1}, a_k).$$

L'unicité de cette représentation découle du fait que des suites distinctes de la forme (13) sont des éléments *distincts* du groupe G.

Soient deux familles de groupes abéliens, $A_1, A_2, \ldots, A_k$ *et* $B_1, B_2, \ldots, B_k$; *si les groupes* A_i *et* B_i *sont isomorphes,* $i = 1, 2, \ldots, k$, *alors les groupes*

$$G = A_1 + A_2 + \ldots + A_k$$

et

$$H = B_1 + B_2 + \ldots + B_k$$

sont aussi isomorphes.

En effet, soit φ_i l'isomorphisme du groupe A_i sur le groupe B_i qui fait correspondre à tout élément a_i de A_i l'élément $a_i\varphi_i$ de B_i; l'application φ associant à tout élément $(a_1, a_2, \ldots, a_k)$ du groupe G l'élément du groupe H, défini par la formule:

$$(a_1, a_2, \ldots, a_k)\varphi = (a_1\varphi_1, a_2\varphi_2, \ldots, a_k\varphi_k),$$

est manifestement un isomorphisme du groupe G sur le groupe H.

Soient $A_1, A_2, \ldots, A_k$ *des groupes abéliens finis dont les ordres sont respectivement* $n_1, n_2, \ldots, n_k$; *alors leur somme directe* G *est un groupe abélien fini d'ordre* n, *où* n *est le produit des ordres des termes directs*:

$$n = n_1 n_2 \ldots n_k. \tag{16}$$

En effet, les suites distinctes de la forme (13), dont la première composante a_1 prend n_1 valeurs distinctes, la seconde composante a_2 prend n_2 valeurs distinctes, etc., sont au nombre de $n = n_1 n_2 \ldots n_k$.

Considérons quelques *exemples.*

Si l'ordre n *d'un groupe cyclique fini* $\{a\}$ *est le produit de deux nombres naturels* s *et* t, *premiers entre eux,*

$$n = st \qquad (s, t) = 1,$$

alors le groupe $\{a\}$ *se décompose en une somme directe de deux groupes cycliques dont les ordres sont respectivement* s *et* t.

Notons additivement le groupe $\{a\}$. Posant $b = ta$, on a

$$sb = (st)\,a = na = 0,$$

et pour $0 < k < s$ on a

$$kb = (kt)\,a \neq 0,$$

c'est-à-dire le sous-groupe cyclique $\{b\}$ est d'ordre s. De même, le sous-groupe cyclique $\{c\}$ de générateur $c = sa$ est d'ordre t. L'intersection $\{b\} \cap \{c\}$ ne contient que l'élément nul, car si l'on avait $kb = lc$ avec $0 < k < s$, $0 < l < t$, alors on aurait

$$(kt)\,a = (ls)\,a,$$

d'où, vu que les entiers kt et ls sont inférieurs à n, on obtiendrait

$$kt = ls\,;$$

or, cela est impossible, les nombres s et t étant premiers entre eux. Enfin, il existe deux entiers u et v tels que l'on ait

$$su + tv = 1,$$

et, par conséquent, on a

$$a = v\,(ta) + u\,(sa) = vb + uc\,;$$

cela signifie que tout élément du groupe $\{a\}$ est une somme des éléments respectivement du sous-groupe $\{b\}$ et du sous-groupe $\{c\}$.

Un groupe abélien G est dit *indécomposable* s'il ne peut pas être décomposé en une somme directe de deux ou plusieurs sous-groupes différents de son sous-groupe nul. Un groupe cyclique fini dont l'ordre est une puissance d'un nombre premier p s'appelle *groupe primaire* associé au nombre premier p (ou, encore, groupe p-primaire). Appliquant à plusieurs reprises la proposition démontrée ci-dessus, nous obtenons le résultat: *tout groupe cyclique fini se décompose en une somme directe de groupes cycliques primaires associés à des nombres premiers distincts.* Plus précisément, *un groupe cyclique d'ordre* n, *avec*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s},$$

où $p_1, p_2, \ldots, p_s$ *sont des nombres premiers distincts, se décompose en une somme directe de* s *groupes cycliques dont les ordres sont respectivement* $p_1^{k_1}, p_2^{k_2}, \ldots, p_s^{k_s}$.

Tout groupe cyclique primaire est indécomposable.

En effet, soit un groupe cyclique fini $\{a\}$ d'ordre p^k, où p est un nombre premier. Si ce groupe était décomposable, alors, d'après

(7), il posséderait des sous-groupes non nuls, dont l'intersection est l'élément nul. Or, en réalité, *tout sous-groupe non nul du groupe en question contient l'élément non nul*

$$b = p^{k-1}a.$$

Pour le démontrer, choisissons un élément non nul x de notre groupe,

$$x = sa, \qquad 0 < s < p^k.$$

On peut mettre le nombre s sous la forme

$$s = p^l s', \qquad 0 \leqslant l < k,$$

avec s' non divisible par p, c'est-à-dire s' et p sont premiers entre eux; par conséquent, il existe deux entiers u et v tels que

$$s'u + pv = 1.$$

Mais alors

$$(p^{k-l-1}u)\,x = (p^{k-l-1}us)\,a = (p^{k-1}us')\,a = p^{k-1}(1 - pv)\,a =$$
$$= (p^{k-1} - p^k v)\,a = p^{k-1}a - v\,(p^k a) = p^{k-1}a = b,$$

c'est-à-dire l'élément b appartient au sous-groupe cyclique $\{x\}$.

Le groupe additif des nombres entiers (c'est-à-dire un groupe cyclique infini) ainsi que le groupe additif des nombres rationnels sont indécomposables.

Ces groupes sont indécomposables, car, pour tout couple d'éléments non nuls de chacun de ces groupes, il existe un multiple commun non nul, c'est-à-dire tout couple de sous-groupes cycliques non nuls de chacun de ces groupes a une intersection non nulle.

Notons que, un groupe abélien G étant noté multiplicativement, on doit, au lieu d'une somme directe, parler d'un *produit direct*.

Le groupe multiplicatif des nombres réels non nuls se décompose en produit direct du groupe multiplicatif des nombres réels positifs et du groupe multiplicatif composé des nombres 1 *et* -1.

En effet, l'intersection des sous-groupes indiqués du groupe en question ne contient que le nombre 1, élément unité du groupe. D'autre part, tout nombre positif est le produit de ce nombre par 1, et tout nombre négatif est le produit de sa valeur absolue par le nombre -1.

§ 67. Groupes abéliens finis

Soit un nombre fini de groupes cycliques primaires dont certains peuvent être associés à un même nombre premier ou bien être d'un même ordre (et, par conséquent, isomorphes); alors leur somme direc-

te est, bien entendu, un groupe abélien fini. Il s'avère qu'on épuise ainsi tous les groupes abéliens finis :

Théorème fondamental des groupes abéliens finis. *Tout groupe abélien fini G, qui n'est pas le groupe nul, se décompose en une somme directe de sous-groupes cycliques primaires.*

On commence la démonstration du théorème par la remarque : *le groupe G possède des éléments non nuls ayant pour ordres des puissances de nombres premiers.* En effet, soit un élément non nul x de G d'ordre l, $lx = 0$; si p^k, $k > 0$, est une puissance du nombre premier p telle que p^k soit un diviseur de l,

$$l = p^k m,$$

alors l'élément mx est non nul et d'ordre p^k.

Soient

$$p_1, p_2, \ldots, p_s \tag{1}$$

tous les nombres premiers *distincts* dont certaines puissances sont les ordres de certains éléments du groupe G. Désignons par p un nombre quelconque de la suite (1) et par P l'ensemble des éléments du groupe G ayant pour ordres les puissances de p.

L'ensemble P est un sous-groupe du groupe G. En effet, P contient l'élément 0, son ordre étant $1 = p^0$. Ensuite, si $p^k x = 0$, alors $p^k(-x) = 0$. Enfin, si $p^k x = 0$, $p^l y = 0$ et, par exemple, $k \geqslant l$, alors on a

$$p^k (x + y) = 0,$$

c'est-à-dire l'ordre de l'élément $x + y$ est soit le nombre p^k, soit un des diviseurs de p^k, autrement dit, une puissance du nombre p.

p parcourant successivement s valeurs (1), nous obtenons s sous-groupes non nuls

$$P_1, P_2, \ldots, P_s. \tag{2}$$

Le groupe G est somme directe de ces sous-groupes,

$$G = P_1 + P_2 + \ldots + P_s. \tag{3}$$

En effet, soit x un élément du groupe G; alors son ordre l n'a d'autres diviseurs que certaines puissances des nombres premiers (1) :

$$l = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s},$$

avec $k_i \geqslant 0$, $i = 1, 2, \ldots, s$. Par conséquent, comme il a été montré à la fin du paragraphe précédent, le sous-groupe cyclique $\{x\}$ se décompose en une somme directe de sous-groupes cycliques primaires dont les ordres sont respectivement $p_1^{k_1}, p_2^{k_2}, \ldots, p_s^{k_s}$. Ces sous-groupes appartiennent aux sous-groupes correspondants

de la famille (2) et, par conséquent, l'élément x est la somme de certains éléments des sous-groupes (2), chaque sous-groupe de la famille (2) ne contenant pas plus d'un élément de la décomposition de x. Ceci démontre l'égalité

$$G = \{P_1, P_2, \ldots, P_s\},$$

analogue à l'égalité (6) du paragraphe précédent.

Pour démontrer l'égalité analogue à l'égalité (7) du paragraphe précédent, fixons un indice i, $2 \leqslant i \leqslant s$. Tout élément y du sous-groupe $\{P_1, P_2, \ldots, P_{i-1}\}$ est de la forme

$$y = a_1 + a_2 + \ldots + a_{i-1},$$

où a_j est un élément du sous-groupe P_j et, par conséquent, d'ordre $p_j^{k_j}$, $j = 1, 2, \ldots, i-1$. Il en résulte que

$$(p_1^{k_1} p_2^{k_2} \ldots p_{i-1}^{k_{i-1}})\, y = 0,$$

c'est-à-dire que l'ordre de l'élément y est un diviseur du nombre $p_1^{k_1}\, p_2^{k_2} \ldots p_{i-1}^{k_{i-1}}$, de sorte que l'élément y, à condition qu'il soit non nul, ne peut pas appartenir au sous-groupe P_i. Ceci démontre que

$$\{P_1, P_2, \ldots, P_{i-1}\} \cap P_i = 0,$$

ce qu'il fallait démontrer.

Un groupe abélien dont chaque élément a pour ordre une puissance d'un même nombre premier p est dit *primaire* associé au nombre p ou, encore, p-primaire. Les groupes cycliques primaires sont un cas particulier de groupes primaires. Ainsi, les sous-groupes de la famille (2) sont primaires. Ils s'appellent *composantes primaires* du groupe G, tandis que la décomposition (3) est dite *décomposition du groupe G en somme directe de composantes primaires*. Les sous-groupes (2) étant bien définis dans le groupe G, il en est de même pour la *décomposition de G en somme directe de composantes primaires*.

Il est clair que la décomposition en somme directe de composantes primaires, qui existe pour tout groupe abélien fini, *ramène la démonstration du théorème fondamental au cas particulier de groupe abélien fini p-primaire P, p étant un nombre premier*. Considérons ce cas.

Soit a_1 un des éléments du groupe P ayant l'ordre le plus élevé. Supposons ensuite qu'il existe des éléments non nuls de P tels que les sous-groupes cycliques engendrés par ces éléments soient disjoints avec le sous-groupe cyclique $\{a_1\}$; notons par a_2 un des éléments jouissant de cette propriété et tel que a_2 soit de l'ordre le plus élevé: aussi on a

$$\{a_1\} \cap \{a_2\} = 0.$$

Supposons que l'on ait déjà choisi les éléments $a_1, a_2, \ldots, a_{i-1}$ satisfaisant à ces conditions. Nous désignerons le sous-groupe du groupe P, engendré par les sous-groupes cycliques des éléments $a_1, a_2, \ldots, a_{i-1}$, par $\{a_1, a_2, \ldots, a_{i-1}\}$,

$$\{\{a_1\}, \{a_2\}, \ldots, \{a_{i-1}\}\} = \{a_1, a_2, \ldots, a_{i-1}\}. \tag{4}$$

Il est clair que ce sous-groupe est composé des sommes de multiples des éléments $a_1, a_2, \ldots, a_{i-1}$; nous dirons que ce sous-groupe est *engendré* par les éléments $a_1, a_2, \ldots, a_{i-1}$. Dans l'ensemble des éléments du groupe P dont les sous-groupes cycliques sont disjoints avec le sous-groupe $\{a_1, a_2, \ldots, a_{i-1}\}$ fixons un élément a_i tel qu'il soit d'ordre le plus élevé; aussi on a

$$\{a_1, a_2, \ldots, a_{i-1}\} \cap \{a_i\} = 0. \tag{5}$$

Le groupe P étant fini, le processus indiqué doit s'arrêter après un nombre fini de pas; supposons qu'il s'arrêtera lorsque nous aurons choisi les éléments $a_1, a_2, \ldots, a_s$. Désignant par P' le sous-groupe engendré par ces éléments,

$$P' = \{a_1, a_2, \ldots, a_s\},$$

ou, encore,

$$P' = \{\{a_1\}, \{a_2\}, \ldots, \{a_s\}\}, \tag{6}$$

le sous-groupe cyclique de tout élément non nul de P a donc l'intersection non nulle avec le sous-groupe P'.

L'égalité (6) et l'égalité (5), valable pour tout i, $i = 2, 3, \ldots, s$, montrent, vu (4), que le *sous-groupe P' est une somme directe des sous-groupes cycliques* $\{a_1\}, \{a_2\}, \ldots, \{a_s\}$,

$$P' = \{a_1\} + \{a_2\} + \ldots + \{a_s\}. \tag{7}$$

Il reste à démontrer qu'en *réalité le sous-groupe P' coïncide avec le groupe P.*

Soit x un élément d'ordre p du groupe P. Etant donné que

$$P' \cap \{x\} \neq 0,$$

et vu que le sous-groupe $\{x\}$ n'a d'autres sous-groupes non nuls que $\{x\}$ (rappelons que l'ordre d'un sous-groupe est un diviseur de l'ordre du groupe et que le nombre p, ordre de $\{x\}$, est premier), il en résulte que, en réalité, le sous-groupe $\{x\}$ appartient au sous-groupe P' et que, par conséquent, x appartient à P'. Ainsi, tout élément d'ordre p du groupe P appartient au sous-groupe P'.

Supposons qu'on ait déjà montré que tout élément du groupe P, dont l'ordre n'est pas supérieur au nombre p^{k-1}, appartient au sous-groupe P'; soit x un élément de P d'ordre p^k. En vertu du choix des éléments $a_1, a_2, \ldots, a_s$, leurs ordres respectifs forment une

suite non croissante, de sorte que l'on peut indiquer un indice i, $1 \leqslant i-1 \leqslant s$, tel que les ordres des éléments $a_1, a_2, \ldots, a_{i-1}$ soient supérieurs ou égaux à p^k et que l'ordre de tout élément a_i avec $i-1 < s$ soit strictement inférieur à p^k, c'est-à-dire inférieur à l'ordre de l'élément x. Vu les conditions imposées au choix de a_i, il en résulte que si

$$Q = \{a_1, a_2, \ldots, a_{i-1}\},$$

alors

$$Q \cap \{x\} \neq 0.$$

Or, on a démontré dans le paragraphe précédent que tout sous-groupe non nul d'un groupe cyclique primaire $\{x\}$ d'ordre p^k contient l'élément

$$y = p^{k-1}x. \tag{8}$$

Donc, l'élément y appartient à l'intersection $Q \cap \{x\}$ et, par conséquent, il appartient au sous-groupe Q. Ceci permet de représenter y sous la forme d'une somme de multiples des éléments $a_1, a_2, \ldots, a_{i-1}$,

$$y = l_1a_1 + l_2a_2 + \ldots + l_{i-1}a_{i-1}. \tag{9}$$

Il découle de (8) que l'élément y est d'ordre p. Ainsi,

$$(pl_1)\,a_1 + (pl_2)\,a_2 + \ldots + (pl_{i-1})\,a_{i-1} = 0,$$

c'est-à-dire, en vertu de l'existence de la décomposition directe (7), on a

$$(pl_j)\,a_j = 0, \qquad j = 1, 2, \ldots, i-1.$$

Donc, le nombre pl_j doit être divisible par l'ordre de l'élément a_j et, par conséquent, par le nombre p^k, d'où il vient que l_j est divisible par p^{k-1},

$$l_j = p^{k-1}m_j, \qquad j = 1, 2, \ldots, i-1. \tag{10}$$

Soit

$$z = m_1a_1 + m_2a_2 + \ldots + m_{i-1}a_{i-1}.$$

z est un élément du sous-groupe Q et, par conséquent, du sous-groupe P' ; en outre, vu (9) et (10), on a

$$y = p^{k-1}z. \tag{11}$$

De (8) et (11) découle l'égalité

$$p^{k-1}(x-z) = 0,$$

c'est-à-dire l'ordre de l'élément

$$t = x - z$$

ne dépasse pas p^{k-1}; par conséquent, en vertu de l'hypothèse de récurrence, t appartient au sous-groupe P'. Aussi l'élément x, en tant que somme de deux éléments de P', $x = z + t$, est un élément du sous-groupe P'. Ceci démontre que tout élément d'ordre p^k du groupe P appartient à P'.

Donc, notre raisonnement qui est basé sur une récurrence sur k, exposant de la puissance p^k, permet d'affirmer que tout élément du groupe P est aussi un élément du sous-groupe P', c'est-à-dire $P' = P$. La démonstration du théorème fondamental est terminée.

Comme corollaire de ce théorème on obtient le résultat: *un groupe abélien fini est un groupe p-primaire si et seulement si son ordre est une puissance du nombre premier p.* En effet, comme on l'a montré , tout groupe abélien fini p-primaire P se décompose en une somme directe de groupes cycliques p-primaires, de sorte que l'ordre du groupe P est le produit des ordres de ces groupes cycliques, c'est-à-dire une puissance du nombre premier p. Inversement, si un groupe abélien fini est d'ordre p^k avec p nombre premier, alors l'ordre de tout élément est un diviseur de p^k, c'est-à-dire une puissance de p, de sorte que le groupe en question est un groupe p-primaire.

Le théorème fondamental ne donne pas encore la solution complète du problème de description des groupes abéliens finis, car on n'a pas encore exclu l'éventualité suivante: les sommes directes de deux familles distinctes de groupes cycliques primaires, associés à des nombres premiers, peuvent être des groupes isomorphes. En réalité, il n'en est pas ainsi, comme le montre le théorème suivant:

Soit un groupe abélien fini G décomposé de deux façons différentes en sommes directes de sous-groupes cycliques primaires:

$$G = \{a_1\} + \{a_2\} + \ldots + \{a_s\} = \{b_1\} + \{b_2\} + \ldots + \{b_t\}; \qquad (12)$$

alors le nombre des termes directs dans les deux décompositions est le même, $s = t$, et l'on peut établir entre les termes directs des deux décompositions une correspondance bijective telle que les termes correspondants soient des groupes cycliques de même ordre, c'est-à-dire qu'ils soient isomorphes.

Remarquons d'abord que groupant dans l'une des décompositions directes (12), par exemple, dans la première, les termes directs associés à un nombre premier donné, soit p, la somme directe de ces termes est un sous-groupe p-primaire du groupe G; de plus, ce sous-groupe est une composante primaire de G, car son ordre est la puissance la plus élevée du nombre p telle qu'elle soit diviseur de l'ordre de G. Groupant de cette manière les termes directs dans chacune des décompositions (12), nous obtenons, dans les deux cas, une décomposition du groupe G en somme directe de composantes primaires, dont l'unicité a été déjà montrée ci-dessus.

Cette remarque permet de ramener la démonstration de notre théorème au cas où *G est un groupe p-primaire*. Supposons que les indices des termes directs dans chacune des décompositions directes (12) soient choisis de manière que leurs ordres respectifs forment une suite non croissante, c'est-à-dire que les éléments a_1, a_2, ..., a_s aient les ordres respectifs

$$p^{k_1},\ p^{k_2},\ \ldots,\ p^{k_s},$$

avec

$$k_1 \geqslant k_2 \geqslant \ldots \geqslant k_s,$$

et que les éléments $b_1, b_2, \ldots, b_t$ aient les ordres respectifs

$$p^{l_1},\ p^{l_2},\ \ldots,\ p^{l_t},$$

avec

$$l_1 \geqslant l_2 \geqslant \ldots \geqslant l_t.$$

Si le théorème n'était pas vrai, on pourrait trouver un indice i, $i \geqslant 1$, tel que l'on aurait

$$k_1 = l_1,\ \ldots,\ k_{i-1} = l_{i-1}, \qquad (13)$$

et

$$k_i \neq l_i.$$

Il est clair que $i \leqslant \min(s, t)$, car les produits des ordres des termes directs des deux décompositions (12) donnent l'ordre du groupe G. Montrons que l'hypothèse que nous venons de faire conduit à l'absurde.

Soit, par exemple

$$k_i < l_i. \qquad (14)$$

Notons par H l'ensemble des éléments du groupe G dont les ordres ne sont pas supérieurs à p^{k_i}. C'est un sous-groupe du groupe G, car, x et y étant deux éléments de H, les éléments $x + y$ et $-x$ ont les ordres qui ne dépassent pas le nombre p^{k_i}.

Notons que le sous-groupe H contient, en particulier, les éléments:

$$p^{k_1-k_i}a_1,\ p^{k_2-k_i}a_2,\ \ldots,\ p^{k_{i-1}-k_i}a_{i-1},\ a_i,\ a_{i+1},\ \ldots,\ a_s.$$

D'autre part, si $1 \leqslant j \leqslant i - 1$, alors l'élément $p^{k_j-k_i-1}a_j$ est d'ordre p^{k_i+1} et, par conséquent, n'appartient pas à H. Il en résulte que la classe d'équivalence $a_j + H$ (rappelons que l'on utilise la notation additive), en tant qu'élément du groupe-quotient G/H, est d'ordre $p^{k_j-k_i}$; ce même nombre $p^{k_j-k_i}$ est l'ordre du sous-groupe cyclique $\{a_j + H\}$. Démontrons que *le groupe G/H est une somme*

directe des sous-groupes cycliques $\{a_j+H\}$, $j=1, 2, \ldots, i-1$,

$$G/H=\{a_1+H\}+\{a_2+H\}+\ldots+\{a_{i-1}+H\}, \tag{15}$$

et que, par conséquent, son ordre est le nombre

$$p^{(k_1-k_i)+(k_2-k_i)+\ldots+(k_{i-1}-k_i)}. \tag{16}$$

Soit x un élément du groupe G; alors il existe pour x une écriture de la forme:

$$x=m_1a_1+m_2a_2+\ldots+m_sa_s.$$

Supposons que pour $j=1, 2, \ldots, i-1$, on ait

$$m_j=p^{k_j-k_i}q_j+n_j,$$

avec

$$0\leqslant n_j<p^{k_j-k_i}. \tag{17}$$

Alors on a

$$m_ja_j=q_j(p^{k_j-k_i}a_j)+n_ja_j,$$

et, vu que le premier terme du second membre appartient à H, on obtient

$$m_ja_j+H=n_ja_j+H.$$

D'autre part, on a

$$m_ia_i+H=H, \ldots, m_sa_s+H=H.$$

Par conséquent, on a

$$\begin{aligned} x+H&=(m_1a_1+H)+(m_2a_2+H)+\ldots+(m_sa_s+H)=\\ &=(n_1a_1+H)+(n_2a_2+H)+\ldots+(n_{i-1}a_{i-1}+H). \end{aligned} \tag{18}$$

Soit une autre écriture de cette forme

$$x+H=(n'_1a_1+H)+(n'_2a_2+H)+\ldots+(n'_{i-1}a_{i-1}+H), \tag{19}$$

avec

$$0\leqslant n'_j<p^{k_j-k_i},\ j=1, 2\ \ldots, i-1. \tag{20}$$

Alors les éléments

$$n_1a_1+n_2a_2+\ldots+n_{i-1}a_{i-1}$$

et

$$n'_1a_1+n'_2a_2+\ldots+n'_{i-1}a_{i-1}$$

appartiennent à une même classe d'équivalence de G modulo H, c'est-à-dire leur différence appartient à H, de sorte que l'on a

$$p^{k_i}[(n_1-n'_1)a_1+(n_2-n'_2)a_2+\ldots+(n_{i-1}-n'_{i-1})a_{i-1}]=0.$$

Il en résulte (vu que la première des décompositions (12) est directe) que

$$p^{k_i}(n_j - n'_j)a_j = 0, \qquad j = 1, 2, \ldots, i-1,$$

et, par conséquent, le nombre $p^{k_i}(n_j - n'_j)$ doit être divisible par l'ordre p^{k_j} de l'élément a_j, de sorte que la différence $n_j - n'_j$ est divisible par le nombre $p^{k_j - k_i}$. Il en découle, vu (17) et (20), que

$$n_j = n'_j, \qquad j = 1, 2, \ldots, i-1,$$

c'est-à-dire que les écritures (18) et (19) sont identiques. Ceci démontre l'existence de la décomposition directe (15).

Des raisonnements analogues appliqués à la seconde décomposition directe (12) démontreront que ce même groupe-quotient G/H admet la décomposition directe

$$G/H = \{b_1 + H\} + \{b_2 + H\} + \ldots + \{b_{i-1} + H\} + \{b_i + H\} + \ldots,$$

c'est-à-dire que, en vertu de (13) et (14), l'ordre de G/H doit être *strictement supérieur* au nombre (16). Cette contradiction démontre le théorème.

Ainsi, nous avons obtenu la description complète des groupes abéliens finis. Notamment, *formons toutes les suites finies de nombres naturels*

$$(n_1, n_2, \ldots, n_k),$$

dont chaque nombre n_j, *différent de l'unité, est une puissance d'un nombre premier, les nombres* n_j *n'étant pas forcément tous distincts. A toute suite ainsi construite faisons correspondre une somme directe de groupes cycliques dont les ordres respectifs sont les nombres naturels de la suite fixée. Les groupes abéliens finis obtenus de cette manière sont non isomorphes deux à deux, tandis que tout groupe abélien fini est isomorphe à l'un de ces groupes.*

INDEX ALPHABÉTIQUE